CA Service Desk Manager

Manuel de mise en oeuvre

Version 12.9.00



La présente Documentation, incluant les systèmes d'aide intégrés et le matériel distribué au format électronique (ci-après nommée "Documentation"), vous est exclusivement fournie à titre d'information et peut être à tout moment modifiée ou retirée par CA.

La présente Documentation ne peut être copiée, transférée, reproduite, divulguée, modifiée ou dupliquée, en tout ou partie, sans autorisation préalable et écrite de CA. Cette Documentation est confidentielle et appartient à CA et ne peut pas être divulguée par vous ou utilisée à d'autres fins que celles spécifiées dans (i) un accord distinct passé entre vous et CA régissant l'utilisation du logiciel CA et auquel la Documentation se rapporte ; ou (ii) un accord de confidentialité distinct passé entre vous et CA.

Nonobstant ce qui précède, si vous êtes titulaire de la licence du ou des produits logiciels décrits dans la Documentation, vous pourrez imprimer un nombre raisonnable de copies de la Documentation relative à ces logiciels pour une utilisation interne par vous-même et par vos employés, à condition que les mentions et légendes de copyright de CA figurent sur chaque copie.

Le droit de réaliser des copies de la Documentation est limité à la période pendant laquelle la licence applicable du logiciel demeure pleinement effective. Dans l'hypothèse où le contrat de licence prendrait fin, pour quelque raison que ce soit, vous devrez renvoyer à CA les copies effectuées ou certifier par écrit que toutes les copies partielles ou complètes de la Documentation ont été retournées à CA ou qu'elles ont bien été détruites.

SOUS RESERVE DES DISPOSITIONS PREVUES PAR LA LOI APPLICABLE, CA FOURNIT LA PRESENTE DOCUMENTATION "TELLE QUELLE" SANS AUCUNE GARANTIE, EXPRESSE OU IMPLICITE, NOTAMMENT AUCUNE GARANTIE DE LA QUALITE MARCHANDE, D'UNE QUELCONQUE ADEQUATION A UN USAGE PARTICULIER OU DE NON-INFRACTION. EN AUCUN CAS, CA NE POURRA ETRE TENU POUR RESPONSABLE EN CAS DE PERTE OU DE DOMMAGE, DIRECT OU INDIRECT, SUBI PAR L'UTILISATEUR FINAL OU PAR UN TIERS, ET RESULTANT DE L'UTILISATION DE CETTE DOCUMENTATION, NOTAMMENT TOUTE PERTE DE PROFITS OU D'INVESTISSEMENTS, INTERRUPTION D'ACTIVITE, PERTE DE DONNEES OU DE CLIENTS, ET CE MEME DANS L'HYPOTHESE OU CA AURAIT ETE EXPRESSEMENT INFORME DE LA POSSIBILITE DE LA SURVENANCE DE TELS DOMMAGES OU PERTES.

L'utilisation de tout produit logiciel mentionné dans la Documentation est régie par le contrat de licence applicable, ce dernier n'étant en aucun cas modifié par les termes de la présente.

CA est le fabricant de la présente Documentation.

Le présent Système étant édité par une société américaine, vous êtes tenu de vous conformer aux lois en vigueur du Gouvernement des Etats-Unis et de la République française sur le contrôle des exportations des biens à double usage et aux autres réglementations applicables et ne pouvez pas exporter ou réexporter la documentation en violation de ces lois ou de toute autre réglementation éventuellement applicable au sein de l'Union Européenne.

Copyright © 2013 CA. Tous droits réservés. Tous les noms et marques déposées, dénominations commerciales, ainsi que tous les logos référencés dans le présent document demeurent la propriété de leurs détenteurs respectifs.

Produits CA Technologies référencés

Ce document fait référence aux marques et produits CA Technologies suivants :

- CA IT Asset Management (anciennement CA Asset Portfolio Management (CA APM))
- CA CMDB
- CA Business Intelligence
- CA Business Service Insight (CA BSI)
- CA Configuration Automation (antérieurement CA Cohesion ACM)
- CA EEM (CA Embedded Entitlements Manager)
- CA Enterprise Workload Automation (CA EWA)
- CA Process Automation (antérieurement CA IT PAM)
- CA Management Database (CA MDB)
- CA Management Portal
- CA Network and Systems Management (CA NSM)
- CA Portal
- CA Remote Control Manager (CA RCM)
- CA Service Desk Manager (CA SDM)
- CA Service Management
- CA Siteminder
- CA Software Delivery
- CA Spectrum® Infrastructure Manager (CA Spectrum)
- CA Wily
- CA Workflow

Informations de contact de CA Technologies

Informations de contact du CA Support

Pour en savoir plus sur les produits CA Technologies destinés aux particuliers, indépendants et entreprises, n'hésitez pas à consulter le site Web de CA Technologies. Vous trouverez les informations suivantes sur notre page www.ca.com/worldwide.

- Informations de contact en ligne et par téléphone de nos services de soutien technique et à la clientèle
- Informations sur les communautés d'utilisateurs et les forums
- Téléchargement de produits et de documentation
- Politique et instructions relatives au CA Support
- Autres ressources utiles pour votre produit

Commentaires sur la documentation des produits

Pour soumettre vos questions et suggestions sur la documentation des produits CA Technologies, envoyez un message à l'adresse techpubs@ca.com.

Pour nous faire parvenir vos commentaires sur la documentation des produits CA Technologies, merci de bien vouloir prendre quelques instants pour remplir notre enquête, également disponible sur le site du CA Support : http://ca.com/docs.

Table des matières

Chapitre 1: Introduction 17

Aperçu 17
Public visé 17
Liste des utilisateurs par défaut de CA SDM 18
Composants de serveur 19

Chapitre 2: Mise à niveau 29

Procédure de planification des mises à niveau de CA SDM 29
- Remarques sur la base de données 31
- Remarques relatives à Gestion des connaissances 34
- Validation du type de document (DocType) 35
- Conservation de vos personnalisations 35
- Remarques sur la migration LREL 40
- Remarques sur la transition d'état 41
- Mise à niveau de la messagerie 42

Fonctionnement de la console Web 44
- Fichier journal de migration 45
- Démarrez la migration manuellement. 45

Mise à niveau de CA CMDB à partir d'une version antérieure 46
Migration de CA SDM r12.9 sur un système d'exploitation Linux/UNIX 64 bits 48
Migration de CA SDM r12.9 sur un système d'exploitation Windows 64 bits 49
Exemple : Migration d'un environnement Windows non pris en charge 49
Exemple : Migration d'un environnement non-Windows non pris en charge 50
Migration de données Automatisation du soutien 51
- Migration d'une base de données Automatisation du soutien 51
- Procédure de conversion des divisions à des clients hébergés 52
- Exportation des données Automatisation du soutien de CA 53
- Importation de données Automatisation du soutien 55
- Configuration de l'accès aux rôles de Automatisation du soutien après la migration 55

Migration d'un univers CA Business Intelligence personnalisé 56
- Sauvegarde d'un univers personnalisé 56
- Installation d'un univers CA Business Intelligence 57
- Mise à jour d'un lien d'univers 57

Configuration après la mise à niveau 58
- Serveurs désactivés autres que les serveurs principaux et secondaires 58
- Prise en charge des clients existants à l'aide du serveur EEM 8.4 58

Mise à niveau de CA Workflow et de CA EEM 58
Conservation de la configuration du processus serveur 60
Activation de CA SDM et intégration de CA IT PAM 60
Nettoyez le moteur Web et le cache du navigateur 61
Configuration du directeur Web et des serveurs 61
LREL post-migration 61
Modification des types d'accès 65
Activer le calcul de la priorité 65
Ajout du champ Priorité de l'incident aux incidents 66
Ajout du champ Urgence aux tickets d'employés 67
Définition des valeurs de ticket pour les utilisateurs du libre-service 67
Activer des transitions d'état 70
Activer des types de transition 71
Personnaliser les domaines d'accès fonctionnel 72
Fichier SITEMODS.JS 74
Ajustez les types d'accès 74
Ajuster les paramètres de partition de données 75
Modifiez les systèmes d'aide après la migration des rôles 76
Paramètres par défaut des contraintes 76
Démarrez l'interface Web IIS (CAisd) 77
Modification des formulaires HTMPL personnalisés 78
Mise à niveau de Gestion des connaissances à partir de r11.2 78
Mise à niveau de Gestion des connaissances à partir de CA SDM r12.x 81

Chapitre 3: Planification 85

Liste des ports par défaut et des ports recommandés CA SDM 85
Procédure de planification de la disponibilité avancée 88
Architecture CA SDM pour la disponibilité avancée 89
Choix de la configuration de disponibilité avancée 91
Remarques sur la configuration de disponibilité avancée 91
Planification de l'installation de CA MDB 99
Remarques relatives à CA MDB 100
Planification de l'installation de CA SDM 102
Remarques relatives à CA SDM 105
Planification de l'installation de CA NSM 116
Planification de l'installation de CA EEM et CA Workflow 116
Remarques relatives à CA EEM 117
Remarques relatives à CA Workflow 118
Planification d'intégration de CA Process Automation 123
Remarques relatives à la sécurité 124
Configuration des communications SSL avec CA Process Automation 124

Planification de l'installation de CA Business Intelligence 127
Remarques relatives au signalement 129
Meilleures pratiques de signalement 133
Stratégies de mise en oeuvre 133
Activer l'authentification Windows dans Firefox 134

Chapitre 4: Installation 137

Mise en oeuvre du logiciel 137
Configuration des serveurs CA SDM 138
Configuration du serveur principal 140
Ajout d'un serveur 140
Configuration des serveurs secondaires 142
Configuration du serveur d'arrière-plan 142
Configuration du serveur de secours ou d'applications 143
Vérification des détails de serveur 145
Procédure de conversion de la configuration conventionnelle en configuration de disponibilité avancée 146
Désactivation de tous les serveurs secondaires 147
Configuration du serveur d'arrière-plan 147
Changement du type de serveur secondaire 148
Configurez les serveurs de secours et d'applications. 148
Vérification des détails de serveur 150
Procédure de conversion de la configuration de disponibilité avancée en conventionnelle 151
Vérifiez la configuration requise. 152
Désactivation de tous les serveurs d'applications et de secours 152
Configuration du serveur principal 153
Vérification des détails du serveur 153
Configuration des serveurs secondaires 154
Vérification des détails de serveur 154
Installation de la CA MDB 155
Installations de MDB 155
Rechercher des informations sur l'intégration et la compatibilité des produit 155
Installation sur SQL Server (Windows) 156
Installation sur Oracle (Windows) 158
Installation sur Oracle (Linux\UNIX) 161
Installation d'une MDB distante sous HP-UX 162
Installation de CA SDM 163
Variables de l'environnement Oracle 164
Installation sur SQL Server (Windows) 164
Installation sur Oracle (Windows) 166
Installation sur Oracle (Linux\UNIX) 169
Configuration du visualiseur 171

Configuration du visualiseur sur un serveur secondaire 171
Configuration des composants de l'Automatisation du soutien 172
Installation de l'Outil de conception Web 177
Installation et configuration de l'intégration de CA SDM et CA NSM 178
Consultation des remarques sur l'intégration 180
Installation du composant d'intégration de CA NSM 181
Convertisseur d'événements CA SDM 184
Consultation des remarques sur la post-intégration 185
Vérification de CA NSM Integration 185
Dépannage de l'intégration de CA NSM 212
Utilisation de l'intégration de CA NSM 217
Installation de CA EEM 224
Installation de CA EEM (Windows) 225
Configuration du kit de développement logiciel de CA EEM en mode de conformité à la norme FIPS 226
Installation de CA EEM (UNIX) 227
Installation de CA Workflow 228
Installation de CA Workflow (Windows) 228
Installation de CA Workflow (UNIX) 229
Installation de l'IDE CA Workflow autonome 229
Désinstallation du client CA Workflow IDE (Windows et Linux) 231
Installation de CA Business Intelligence pour CA SDM 231
Planification de l'installation de CA Business Intelligence 232
Installation de CA Business Intelligence 233
Vérification de l'installation de CA Business Intelligence 234
Vérification de l'installation 235
Fichier journal d'installation 236

Chapitre 5: configuration 237

Configuration du produit 237
Configuration des composants de CA SDM 238
Configuration du journal de vérification de CA CMDB 239
Intégration de CA Cohesion ACM avec CA CMDB 239
Configuration du visualiseur CA CMDB pour AIX 240
Modification des scripts tiers pour la compatibilité de CA CMDB 240
Permutation du serveur cible pour les rapports de CA CMDB 241
Configuration de l'interface Web 241
Ajout de moteurs Web ou de directeurs Web 242
Configuration de l’interface Web 245
Démarrage de l'interface Web 246
Mise en oeuvre de CA Business Intelligence pour CA SDM 247
Vérification des configurations requises 249

Configuration de CA Business Intelligence. 249
Vérification des rapports 267
Configuration de l'authentification Windows intégrée pour CA SDM 268
Vérification de la configuration requise 269
Configuration d'IIS pour IWA 270
Configuration de CA SDM pour IWA 271
Test d'IWA 272
Exécution des politiques d'automatisation 272
Exécution de la fiche de rapport des connaissances. 273
Importation d'exemples de données Gestion des connaissances 274
Configuration du moteur de recherche 275
pdm_k_reindex : utilitaire de réindexation des connaissances 275
Nouvelles balises pour configurer un serveur de domaine pour le robot d'indexation de surface 277
Configuration de CA Workflow 277
Démarrage et arrêt de CA Workflow 278
Configuration de la connexion automatique (Authentification externe) 282
Configuration de la liste de travail et du gestionnaire de flux de travaux pour la connexion automatique 283
Configuration de CA Workflow Design Environment pour la connexion automatique 284
Options CA Workflow 285
Configuration de l'exemple de flux de travail de gestion des problèmes 286
Configuration du flux de travaux de commande de PC 288
Modifier la définition de processus de gestion des changements - Exemple 290
Configuration de l'intégration des flux de travaux CA Process Automation 293
Vérifier les installations de CA Process Automation et de CA SDM 294
Configurer les options de flux de travaux de CA Process Automation 294
Administration utilisateur de CA Process Automation 298
Prise en charge de l'authentification unique de CA SDM vers CA Process Automation en utilisant CA EEM 299
Configuration de la connexion automatique (Authentification de CA MDB) 301
Configurer un point d'entrée unique 302
Mise en oeuvre de l'hébergement multiclient 303
Hébergement multiclient 305
Mise en oeuvre de l'hébergement multiclient 310
Activez Multi-Tenancy 323
Exportation et importation des données du client hébergé 331
Utilitaires utilisés pour l'hébergement multiclient. 334
Procédure d'activation du basculement automatique 342

Chapitre 6: Personnalisation 347

Chapitre 7: Aperçu de la personnalisation 349

Déplacement du module d'authentification vers un serveur externe 350
Vérifiez la configuration requise. 352
Configuration de CA SDM pour l'utilisation de l'authentification externe 353
Procédure de redémarrage des serveurs CA SDM 354
Vérification de l'authentification 357
Personnalisation de méthode de notification 357
Processus de notification 358
Variables de méthode de notification 358
Création d'une méthode de notification personnalisée 363
Personnalisation des requêtes et messages 366
Requêtes de tableau d'affichage 367
Requêtes spécifiques à ITIL 374
Personnalisation des messages de notification d'activité 375
Personnalisation de l'interface Web 381
Personnalisation de schémas à l'aide de l'Outil de conception Web 382
Personnalisation de l'interface Web à l'aide de l'Outil de conception Web 401

Chapitre 8: Modification de liste de grilles de données dans un formulaire de liste 421

Modèles HTML (Formulaire HTMPL) 426
Balises HTMPL 431
Variables serveur 453
Opérations de serveur prises en charge 459
Personnalisation avancée 468

Chapitre 9: Personnalisation du stockage des données du journal d'événements 497

Personnalisation des Rapports CA Business Intelligence 499
Infrastructure de CA Business Intelligence 500
Environnement de développement 501
Environnement 503
Modifications de schéma dans l'Infrastructure 506
Structures de dossiers et de rapports 509
Déplacer des nouveaux rapports Crystal dans CA Business Intelligence 513
Déplacement des rapports d'accès existants dans CA Business Intelligence 515
Déplacement du développement à la production 515
Personnalisation des rapports hérités 516

Conception de rapport personnalisés 517
Génération de rapports 525
Référence d'un modèle de rapport 526
Personnalisation des rapports Crystal 541

Chapitre 10: Remplissage de CA CMDB 543

Remplissage de la base de données 543
Remplissage du chargeur général de ressources de la base de données (GRLoader) 543
Utilisation du chargeur général de ressources pour importer des données 544
Affectations de classe et de famille 544
Chargement de données CA APM 545

Chapitre 11: Utilisation du lanceur RDG (référentiel de données de gestion) 547

Lanceur RDG 547
Terminologie RDG 548
Mappage RDG 549
Lancement RDG 550
Visionneuse CMDBf 550
Définition d'un RDG dans CA CMDB 550
Définitions de l'URL RDG 554
URL de lancement du RDG 555
Paramètres pour la substitution de l'URL 557
Federation et le chargeur général de ressources 559
Fédération d'un CI 559
Définition de plusieurs RDG pour un CI au moyen du chargeur général de ressources 560
Mappage des CI RDG et des CI CA CMDB 561
Configuration des RDG pour la visionneuse CMDBf 563
Lancement de l'interface de navigateur Web RDG 563
Intégration CA Cohesion 564

Chapitre 12: Gestion des services Web 565

Gestion des services Web 565
Composants CA SDM 566
Conseils pour les clients des services Web SOAP 566
Clients Java 567
Configuration des services Web SOAP 569
Redéploiement des services Web 570
Sécurité des services Web 571
Traitement des erreurs SOAP 573
Erreurs de verrouillage 574

Temporisations 575
Codes d'erreur 575
Installation des services Web 577
Activation de la phase de conception 577
Caractéristiques externes 577
Authentification d'accès utilisateur 578
Authentification par Nom d'utilisateur/Mot de passe 578
Authentification par l'entremise d'une infrastructure de clés publiques (PKI) 579
Session et autorisation 585
Gestion et contrôle d'accès 586
Objets 597
Mise en cache et mises à jour du système 598
Catégories et propriétés 599
Renvois d'objets XML 600
méthodologie ITIL 602
Création d'incident ou de problème 602
Requête pour les incidents ou les problèmes 603
Attachement d'un incident à un problème 604
Association d'un problème à une demande de changement 604
Eléments de configuration 604
Utilisation des services Web 605
Connexions 605
Exécution des tâches communes 605
REST et SOAP 609
Sécurité REST 610
Options du service Web 612

Chapitre 13: Intégration à d'autres produits 615

Intégration de CA Workflow 615
Composants de CA Workflow 616
Accès à CA Workflow 618
Intégration CA Portal 620
Vérification de l'accessibilité à l'interface Web CA SDM 620
Installation et démarrage de CA Portal 621
Configuration de CA SDM pour utiliser SSL avec CA Portal 623
Intégration des produits d'ordinateur central 627
Charger les données côté serveur CA SDM 628
Produits CA utilisant actuellement CAISDI 628
Produits CA susceptibles d'utiliser CAISDI 629
Intégration de CA Business Service Insight 630
Affichage des informations de CA BSI dans CA SDM 632

Chapitre 14: Répertoire Samples 637

Contenu du répertoire Samples 637
- Modification du catalogue de messages 637
- call_mgt 638
- data 639
- macro_lock 639
- hébergement multiclient 639
- pdmconf 640
- signalement 640
- sdk 640
- vues 641

Chapitre 15: Chargement de contenu supplémentaire 643

sd_content.dat 643

Chapitre 1: Introduction

Ce chapitre traite des sujets suivants :

Aperçu (page 17)
Public visé (page 17)
Liste des utilisateurs par défaut de CA SDM (page 18)
Composants de serveur (page 19)

Aperçu

Ce manuel vous fournit les informations dont vous avez besoin pour réussir la mise en oeuvre de CA SDM dans votre entreprise, notamment des informations sur les opréations suivantes :

- Planification et préparation pour une nouvelle installation ou une mise à niveau
- Installation et mise à niveau de tous les composants nécessaires du produit
- Configuration des composants du produit
- Intégration à certains produits CA Technologies

  Remarque : Ce manuel ne détaille *pas* les intégrations à tous les produits CA Technologies. Pour des informations détaillées sur les intégrations à CA SDM non décrites dans ce manuel, reportez-vous au *Livre vert CA Unicenter Service Desk Integrations* à l'adresse http://www.ca.com/worldwide.

Remarque : Vous trouverez la version la plus récente des Notes de parution, qui contiennent la configuration système requise, ainsi que le fichier Readme facultatif (si disponible) à l'adresse http://www.ca.com/worldwide.

Public visé

Ce manuel est destiné aux personnes souhaitant des informations sur l'installation, la mise à niveau et la configuration de CA SDM. Les utilisateurs suivants ont des tâches spécifiques à effectuer à l'aide des informations de ce guide :

- Les *administrateurs système* et les *administrateurs* utilisent les informations de ce manuel, ainsi que leur connaissance du système d'exploitation, pour installer le produit, le mettre à niveau d'une version vers une autre et le configurer selon vos exigences de mise en oeuvre.

- Les *intégrateurs* utilisent les informations de ce manuel et leur connaissance des produits CA Technologies pour intégrer CA SDM avec d'autres produits CA Technologies.

  Remarque : Ce manuel ne détaille *pas* les intégrations à tous les produits CA Technologies. Pour des informations détaillées sur les intégrations à CA SDM non décrites dans ce manuel, reportez-vous au *Livre vert CA Unicenter Service Desk Integrations* à l'adresse http://www.ca.com/worldwide.

- Les *utilisateurs* peuvent, le cas échéant, utiliser les informations de ce manuel pour installer le produit et ses composants.

Pour utiliser les informations de ce manuel, vous devez avoir :

- Une connaissance pratique des systèmes d'exploitation Windows ou UNIX, selon votre environnement de production actuel.
- La capacité d'effectuer des tâches d'administration de base sur votre système d'exploitation.
- Selon votre environnement de travail, il se peut que vous deviez avoir des connaissances sur les ordinateurs centraux, les dispositifs mobiles et les installations sur serveur.

Remarque : Vous trouverez tout au long de ce manuel des références à NX_ROOT. Ces références concernent la variable d'environnement contenant le chemin d'accès d'installation de CA SDM. Cette variable NX_ROOT est définie dans le fichier de configuration NX.env permettant de définir des variables d'environnement d'CA SDM.

Exemple de définition de NX_ROOT

```
@NX_ROOT=C:\Program Files\CA\Service Desk Manager
```

Liste des utilisateurs par défaut de CA SDM

La liste suivante répertorie les informations sur les utilisateurs par défaut pour les mises en oeuvre typiques de CA SDM :

Système d'exploitation	Produit	Nom d'utilisateur par défaut	Niveau SE ?	Création
Windows	CA SDM	ServiceDesk	Oui	Automatiquement
	CA EEM	Admin Eiam		Mot de passe par défaut : EiamAdmin
	CA MDB SQL Server	ServiceDesk	Non	Créé dans la MDB pendant la configuration

Système d'exploitation	Produit	Nom d'utilisateur par défaut	Niveau SE ?	Création
	CA MDB Oracle	mdbadmin	Non	Créé dans la MDB pendant la configuration
UNIX	CA SDM	srvcdesk	Oui	Créée manuellement
	CA MDB Oracle	mdbadmin	Non	Créé dans la MDB pendant la configuration
Linux	CA SDM	srvcdesk	Oui	Créée manuellement
	CA MDB Oracle	mdbadmin	Non	Créé dans la MDB pendant la configuration

Composants de serveur

CA SDM inclut des composants qui fonctionnent conjointement et sont exécutés sur différents serveurs, en fonction de la configuration du produit. Avant de commencer votre mise en oeuvre, vous devez avoir une compréhension de base des composants suivants :

Gestionnaire de démons (pdm_d_mgr)

Démarre les ensembles de processus tels que définis dans le fichier de démarrage, pdm_startup. Par défaut, le gestionnaire de démons essaie de démarrer jusqu'à 10 fois un composant en échec. Pour vérifier l'état de tous les composants CA SDM, utilisez l'utilitaire pdm_status. L'utilitaire pdm_d_refresh demande au gestionnaire de démons de démarrer un nouveau cycle de 10 tentatives de démarrage d'un processus marqué comme en échec.

Le gestionnaire de démons est exécuté sur tous les serveurs CA SDM.

Répartiteur de messages (sslump_nxd)

Agit comme un bus commun ou un système de transmission de messages. Les composants devant communiquer entre eux s'enregistrent tout d'abord auprès du répartiteur de messages. Lorsqu'un composant envoie un message, le répartiteur de messages le livre aux composants qui se sont enregistrés pour recevoir ce type de message. Si deux composants communiquent tellement qu'il serait inefficace de transmettre les messages par l'entremise du répartiteur de messages, il est préférable de créer un canal rapide entre ceux-ci. Vous pouvez afficher une liste des composants enregistrés à l'aide de l'utilitaire *slstat*.

Le répartiteur de messages est exécuté sur les serveurs suivants, selon la configuration de CA SDM :

- Conventionnelle : serveur principal
- Disponibilité avancée : tous les serveurs

Agent de base de données (platform_agent)

Exécute des requêtes SQL sur la base de données. Les agents de base de données respectent le schéma logique de CA SDM et convertissent le SQL de ce niveau en SQL de plate-forme de base de données physique.

Remarque : L'agent de base de données détecte les déconnexions momentanées et les échecs de requêtes, puis tente de se reconnecter et de communiquer avec la base de données. Ceci n'est destiné qu'aux interruptions courtes (brève interruption du réseau, déconnexion momentanée, etc.). Les interruptions de longue durée telles que l'arrêt d'un service de base de données pour maintenance, etc., ne sont pas couvertes. L'agent ne tentera une nouvelle connexion qu'un certain nombre de fois (la valeur par défaut est de 3 fois) et uniquement sur une courte période de quelques minutes. Si l'interruption dure plus longtemps que quelques minutes, l'agent arrêtera ses tentatives de connexion et CA SDM devra être recyclé une fois la base de données à nouveau accessible.

L'agent de base de données est exécuté sur les serveurs suivants, selon la configuration de CA SDM :

- Conventionnelle : serveur principal
- Disponibilité avancée : tous les serveurs

Fournisseur d'agents (platform_prov_nxd)

Démarre ou arrête les agents de base de données. Par défaut, un certain nombre d'agents sont en cours d'exécution. Si des agents supplémentaires sont nécessaires pour traiter le nombre de requêtes de base de données, le fournisseur d'agents les démarre. Si le système n'a plus besoin d'autant d'agents de base de données, le fournisseur d'agents arrête les agents inutiles.

Le fournisseur d'agents est exécuté sur les serveurs suivants, selon la configuration de CA SDM :

- Conventionnelle : serveur principal
- Disponibilité avancée : tous les serveurs

Base de données virtuelle (bpvirtdb_srvr)

Permet le fonctionnement de plusieurs gestionnaires d'objets. Tous les gestionnaires d'objets qui s'exécutent sur des serveurs principaux ou secondaires se connectent à la base de données virtuelle, qui gère leur accès aux agents de base de données. Par exemple, lors de la récupération d'une nouvelle plage de numéros de référence de tickets, la base de données virtuelle permet de garantir qu'un seul gestionnaire d'objets accède à la table contenant les numéros de référence. La base de données virtuelle effectue également la mise en cache des informations de base de données pour les gestionnaires d'objets.

La base de données virtuelle est exécutée sur les serveurs suivants, selon la configuration de CA SDM :

- Conventionnelle : serveur principal
- Disponibilité avancée : tous les serveurs

Archivage et purge continus (arcpur_srvr)

Exécute vos règles d'archivage et de purge comme configuré par l'administrateur CA SDM.

L'archivage et la purge continus sont exécutés sur les serveurs suivants, selon la configuration de CA SDM :

- Conventionnelle : serveur principal
- Disponibilité avancée : serveur d'arrière-plan

Moniteur de base de données (dbmonitor_nxd)

Contrôle les modifications apportées aux tables communes dans CA MDB, par exemple *ca_contact*.

Le moniteur de base de données est exécuté sur les serveurs suivants, selon la configuration de CA SDM :

- Conventionnelle : serveur principal
- Disponibilité avancée : serveur d'arrière-plan

Démon de courriel (pdm_mail_nxd)

Envoie des notifications par courriel sortantes.

Le démon de courriel est exécuté sur les serveurs suivants, selon la configuration de CA SDM :

- Conventionnelle : serveur principal
- Disponibilité avancée : tous les serveurs

Interface de lecture du courrier entrant (pdm_maileater_nxd)

Accepte les courriels entrants pour la création et la mise à jour de tickets.

Le démon d'interface de lecture du courrier entrant est exécuté sur les serveurs suivants, selon la configuration de CA SDM :

- Conventionnelle : serveur principal
- Disponibilité avancée : serveur d'arrière-plan

Gestionnaire de notifications (bpnotify_nxd)

Gère les notifications dans un environnement Windows. Le gestionnaire de notifications est exécuté sur les serveurs suivants, selon la configuration de CA SDM :

- Conventionnelle : serveur principal
- Disponibilité avancée : serveurs d'applications, d'arrière-plan et de secours

Vérificateur orthographique (lexagent_nxd)

Effectue la vérification orthographique à la demande des clients. Le vérificateur orthographique est exécuté sur tous les serveurs CA SDM.

Démon API de texte (pdm_text_nxd)

Crée et met à jour les tickets par l'entremise d'interfaces externes, telles que la ligne de commande et la messagerie. Le démon API de texte est exécuté sur tous les serveurs CA SDM.

Événement prévu (animator_nxd)

Exécute les délais d'événements. Dans une mise en oeuvre comportant de nombreux types de services ou de contrats, il se peut que de nombreux événements soient actifs et nécessitent un suivi par le moteur Evénement planifié. Dans ce cas, le gestionnaire d'objets du serveur principal doit être consacré exclusivement au moteur Evénement planifié. Vous pouvez configurer d'autres gestionnaires d'objets sur les serveurs principaux ou secondaires pour un accès approprié au produit.

Le démon Événement prévu est exécuté sur les serveurs suivants, selon la configuration de CA SDM :

- Conventionnelle : serveur principal
- Disponibilité avancée : serveur d'arrière-plan

Délai avant violation (ttv_nxd)

Calcule les délais prévus avant violation pour les différents types de service. Le démon Délai avant violation est exécuté sur les serveurs suivants, selon la configuration de CA SDM :

- Conventionnelle : serveur principal
- Disponibilité avancée : serveur d'arrière-plan

Démon de l'utilitaire de surveillance (pdm_proctor_nxd)

(Windows uniquement) Démarre et redémarre les composants CA SDM, comme indiqué par le gestionnaire de démons, sur les serveurs principal et secondaire. Lorsque vous installez un serveur secondaire, le processus *pdm_proctor_nxd* est installé comme service d'utilitaire de surveillance de démon distant CA SDM. Lorsque le serveur principal démarre, le gestionnaire de démons demande à l'utilitaire de surveillance de démon distant de se connecter au répartiteur de messages. Le gestionnaire de démons demande ensuite à l'utilitaire de surveillance de démon distant de démarrer les composants sur le serveur secondaire comme défini par les ensembles de processus dans le fichier de démarrage *pdm_startup*. Dans une configuration de disponibilité avancée, le démon de l'utilitaire de surveillance est exécuté sur tous les serveurs CA SDM.

Gestionnaire d'objets (domsrvr).

Agit comme le processus serveur de CA SDM. Lorsque vous installez un serveur principal, par défaut, deux gestionnaires d'objets sont installés : l'un pour les connexions au produit et l'autre consacré à l'Outil de conception Web. Ceci vous permet de tester vos modifications sans affecter l'environnement de production. Lorsque vous installez un serveur secondaire, vous pouvez configurer des gestionnaires d'objets supplémentaires.

Il doit toujours y avoir un gestionnaire d'objets par défaut s'exécutant sur le serveur principal auquel les clients tels que le moteur Evénement planifié peuvent se connecter.

Le gestionnaire d'objets met également en cache divers enregistrements et diverses tables pour les clients. Si vous utilisez *pdm_userload* pour manipuler ces enregistrements, vous pouvez également utiliser l'utilitaire *pdm_cache_refresh* pour que le gestionnaire d'objets récupère les nouvelles données.Dans une configuration de disponibilité avancée, le gestionnaire d'objets est exécuté sur tous les serveurs CA SDM.

Moteur de méthodes (spel_srvr)

Exécute le code SPEL, l'événement, les macros, etc. pour un gestionnaire d'objets. Nous recommandons d'exécuter chaque gestionnaire d'objets avec son propre moteur de méthode.

Le moteur de méthodes est exécuté sur tous les serveurs CA SDM.

Serveur de connexion (boplgin)

Gère les sessions d'utilisateurs authentifiés.

Le serveur de connexion est exécuté sur les serveurs suivants, selon la configuration de CA SDM :

- Conventionnelle : serveur principal
- Disponibilité avancée : tous les serveurs

Base de données virtuelle LDAP (ldap_virtdb)

Etablit l'interface avec un répertoire LDAP. Le moteur de méthode est exécuté sur les serveurs suivants, selon la configuration de CA SDM :

- Conventionnelle : serveur principal ou secondaire
- Disponibilité avancée : serveur d'arrière-plan ou d'applications

Démon du moteur de recherche Gestion des connaissances (bpebr_nxd)

Effectue des recherches dans la base de connaissances. Au démarrage de CA SDM, le démon bpebr_nxd met les données de documents de connaissances en cache dans sa mémoire à partir de la base de données. Avec une grande base de documents, il se peut que vous rencontriez des problèmes de ressources mémoire. Le démon bpebr_nxd présente les exigences de taille suivantes.

Moteur de recherche Gestion des connaissances

- 100 000 documents
- Taille de la mémoire = 332 000 Ko

Le démon de gestion des connaissances est exécuté sur les serveurs suivants, selon la configuration de CA SDM :

- Conventionnelle : serveur principal ou secondaire
- Disponibilité avancée : serveur d'arrière-plan

Démon d'indexation de la Gestion des connaissances (bpeid_nxd)

Etablit l'index de la base de connaissances.

Le démon d'index de mot clé est exécuté sur les serveurs suivants, selon la configuration de CA SDM :

- Conventionnelle : serveur principal ou secondaire
- Disponibilité avancée : serveur d'arrière-plan

Démon d'évaluation FAQ des Gestion des connaissances (bu_daemon)

Calcule les évaluations FAQ pour Gestion des connaissances. Il est exécuté sur les serveurs suivants selon la configuration de CA SDM :

- Conventionnelle : serveur principal ou secondaire
- Disponibilité avancée : serveur d'arrière-plan

Démon de fiche de rapport des connaissances (krc_daemon)

Effectue des calculs pour la fonction de carte de rapport des connaissances (KRC) des Gestion des connaissances. Cette fonction permet aux analystes et aux gestionnaires d'afficher les différentes vues de matrice de leurs contributions de connaissances et fournissent des commentaires sur les documents les plus efficaces. Les informations fournies peuvent être utilisées de diverses manières pour améliorer les processus de création de documents de connaissances et fournir le meilleur soutien aux clients.

Le démon de fiche de rapport des connaissances est exécuté sur les serveurs suivants, selon la configuration de CA SDM :

- Conventionnelle : serveur principal ou secondaire
- Disponibilité avancée : serveur d'arrière-plan

Démon Gestion des connaissances (kt_daemon)

Gère l'administration de la base de connaissances et la logique de gestion des connaissances. Il gère également les notifications et le processus d'approbation des documents. Le démon de gestion des connaissances est exécuté sur tous les serveurs CA SDM.

Démon de référentiels (rep_daemon)

Gère les référentiels de pièces jointes pour CA SDM et le démon des Gestion des connaissances/de la recherche par mot clé. Le démon de référentiel est exécuté sur les serveurs suivants, selon la configuration de CA SDM :

- Conventionnelle : serveur principal ou secondaire
- Disponibilité avancée : tous les serveurs

Démon de contrôle de version (pdm_ver_nxd)

Synchronise les fichiers de schéma entre un serveur principal et un serveur secondaire pour s'assurer qu'ils utilisent le même schéma. Le démon de contrôle de version est exécuté sur les serveurs suivants, selon la configuration de CA SDM :

- Conventionnelle : serveur principal
- Disponibilité avancée : serveur d'arrière-plan

Serveur Web Apache Tomcat (javaw)

Permet de mettre en oeuvre certaines fonctions, que Microsoft Internet Information Server (IIS) soit utilisé ou non comme serveur Web pour accéder à CA SDM. Ces fonctions incluent CA Workflow, les éléments graphiques, les pièces jointes et les services Web.

Le serveur Web Apache Tomcat peut être administré avec le contrôleur Apache Tomcat (*pdm_tomcat_nxd*). Le serveur Web Apache Tomcat est exécuté sur tous les serveurs CA SDM.

Moteur Web (webengine)

Se connecte aux navigateurs Web par l'entremise d'une commande *pdmweb cgi* s'exécutant sur un serveur Web Microsoft IIS ou Apache Tomcat. Au moins un moteur Web doit être disponible pour l'outil de conception Web sur les serveurs suivants, selon la configuration de CA SDM.

Conventionnelle : serveur principal

Disponibilité avancée : serveurs d'applications, de secours et d'arrière-plan

Ce processus permet au concepteur de schémas de l'outil de conception Web d'écrire des fichiers de schéma. Les moteurs Web sont le véritable client d'un gestionnaire d'objets utilisé par le navigateur Web pour accéder au produit.

Les moteurs Web mettent en cache les formulaires Web .htmpl pour les utilisateurs connectés. Vous pouvez manipuler le cache à l'aide de l'utilitaire *pdm_webcache* et afficher les statistiques de connexion à l'aide de l'utilitaire *pdm_webstat*. Le moteur Web est exécuté sur tous les serveurs CA SDM.

Intermédiaire RF (pdm_rfbroker_nxd)

(applicable à la configuration de disponibilité avancée uniquement). Il gère les rôles des serveurs et les contrôles dans la configuration. Ce démon est exécuté sur tous les serveurs dans la configuration de disponibilité avancée. Il est chargé de collecter des données sur les serveurs d'arrière-plan et de secours et de mettre à jour les renseignements (tels que l'ID de slump, le nom du noeud, le type de serveur) dans la classe ServerStatusMonitor. Il reçoit des messages de diffusion des changements d'état de serveur, met au repos des demandes et enregistre des messages SLUMP_NODE_GONE qu'il transmet aux objets ServerStatusMonitor lorsque le noeud défaillant est le serveur d'arrière-plan. Ce démon n'est pas applicable à la configuration conventionnelle.

Authentification de l'utilisateur connecté (bopauth_nxd)

Effectue la validation du compte utilisateur du système d'exploitation et les recherches d'enregistrement de contact à l'aide du champ Connexion au système pour faire correspondre un utilisateur et un type d'accès.

Si votre entreprise fournit CA SDM à d'autres entreprises clientes, vous pouvez placer le serveur de connexion sur un serveur secondaire sur un site client unique. L'authentification externe peut alors être activée dans les types d'accès. Ceci évite la création de comptes utilisateur pour vos clients sur vos systèmes commerciaux. Il est exécuté sur les serveurs suivants, selon la configuration de CA SDM :

- Conventionnelle : serveur principal ou secondaire (s'il est configuré)
- Disponibilité avancée : serveur d'arrière-plan ou d'applications (s'il est configuré)

Enregistreur périodique (pdm_intrvlog_nxd)

Il rassemble les renseignements de débogage pour déboguer le système. Il est exécuté sur tous les serveurs CA SDM.

Démon QRY KPI (kpi_qry_daemon)

Exécute des requêtes SQL pour mettre à jour des indicateurs clés de performance dans la base de données. Le démon QRY KPI est exécuté sur les serveurs suivants, selon la configuration de CA SDM :

- Conventionnelle : serveur principal
- Disponibilité avancée : serveur d'arrière-plan

Démon SYS KPI (kpi_sys_daemon)

Il collecte des indicateurs clés de performance de type système et les écrit dans la base de données. Le démon SYS KPI est exécuté sur les serveurs suivants, selon la configuration de CA SDM :

- Conventionnelle : serveur principal
- Disponibilité avancée : tous les serveurs

Confirmation de base de données (confirm_db)

Il s'agit d'un utilitaire permettant de vérifier l'accès à la base de données. Il est exécuté sur tous les serveurs CA SDM.

Dictionnaire de données (ddictbuild)

Il s'agit d'un utilitaire permettant de créer le dictionnaire de données. Il est exécuté sur tous les serveurs CA SDM.

Définition de fichier journal (pdm_logfile)

Il s'agit d'un utilitaire permettant de définir les limites de la taille du fichier journal. Il est exécuté sur tous les serveurs CA SDM.

Gestionnaire de rapports (pcrpt_nxd)

Il s'agit d'un utilitaire pour le signalement PC. Il est exécuté sur tous les serveurs CA SDM.

Serveur RPC (rpc_srvr)

Il est utilisé pour effectuer des appels sortants de service Web SOAP. Il est exécuté sur tous les serveurs CA SDM.

CA SA Tomcat (sa_tomcat)

CA SA Tomcat est utilisé pour automatiser le soutien. Il est configuré sur le serveur CA SDM de votre choix.

CAWF Tomcat (cawf_tomcat)

Il s'agit d'une instance Tomcat utilisée pour exécuter CA Workflow. Vous pouvez la configurer sur le serveur CA SDM de votre choix.

Tomcat du visualiseur (viz_tomcat)

Il s'agit d'une instance Tomcat utilisée pour exécuter le visualiseur. Vous pouvez la configurer sur les serveurs suivants, selon la configuration de CA SDM :

- Conventionnelle : tous les serveurs
- Disponibilité avancée : serveur d'applications

Gestionnaire d'événements (ehm_nxd)

Le gestionnaire d'événements gère les événements provenant de CA NSM. Le gestionnaire d'événements est exécuté sur les serveurs suivants, selon la configuration de CA SDM :

- Conventionnelle : serveur principal
- Disponibilité avancée : serveur d'arrière-plan

Démon d'indexation Gestion des connaissances (bpeid_nxd)

Il est chargé d'indexer les documents de connaissances. Il est exécuté sur les serveurs suivants selon la configuration de CA SDM :

- Conventionnelle : serveur principal
- Disponibilité avancée : serveur d'arrière-plan

Serveur d'enregistrement (mdb_registration_nxd)

Il s'agit d'un agent de traitement des demandes d'enregistrement dans la MDB. Le serveur d'enregistrement est exécuté sur les serveurs suivants, selon la configuration de CA SDM :

- Conventionnelle : serveur principal
- Disponibilité avancée : tous les serveurs

Chapitre 2: Mise à niveau

Ce chapitre traite des sujets suivants :

Procédure de planification des mises à niveau de CA SDM (page 29)
Fonctionnement de la console Web (page 44)
Mise à niveau de CA CMDB à partir d'une version antérieure (page 46)
Migration de CA SDM r12.9 sur un système d'exploitation Linux/UNIX 64 bits (page 48)
Migration de CA SDM r12.9 sur un système d'exploitation Windows 64 bits (page 49)
Exemple : Migration d'un environnement Windows non pris en charge (page 49)
Exemple : Migration d'un environnement non-Windows non pris en charge (page 50)
Migration de données Automatisation du soutien (page 51)
Migration d'un univers CA Business Intelligence personnalisé (page 56)
Configuration après la mise à niveau (page 58)

Procédure de planification des mises à niveau de CA SDM

Vérifiez la remarque sur la planification suivante pour la mise à niveau de CA SDM :

- CA SDM prend en charge la mise à niveau des versions r11.2, r12.0, r12.1, r12.5, r12.6 et r12.7 vers la version r12.9 sur toutes les plates-formes prises en charge. Sous Windows, vous pouvez effectuer directement une mise à niveau vers CA SDM r12.9 à partir de r11.2, r12.0, r12.1, r12.5, r12.6 et r12.7.
- Si vous avez installé CA SDM sous Linux ou UNIX, la mise à niveau à partir des versions antérieures à r12.5 vers CA SDM r12.9 se déroule en plusieurs étapes. Si votre installation est exécutée avec une version antérieure du produit (par exemple : r11.2, r12.0 ou r12.1) sous Linux/UNIX, vous devez exécuter le script de mise à niveau automatisée pour CA SDM r12.5 et déplacer CA SDM vers une plate-forme et une base de données prises en charge avant d'exécuter le script de mise à niveau automatisée pour <uskd> r12.9. Si vous disposez de personnalisations, vous devez les appliquer une seule fois, à l'issue de l'exécution du dernier script de mise à niveau automatisée vers r12.9.
- Si vous disposez d'une version antérieure du produit, telle qu'Unicenter Service Desk r6.0 ou r11.1, vous *devez* effectuer une mise à niveau vers CA SDM r11.2 avant d'effectuer la mise à niveau vers CA SDM r12.9.
- Si vous avez ajouté manuellement des variables au fichier NX.env avant la migration, ajoutez-les de nouveau, une fois la migration terminée.

- CA SDM prend uniquement en charge ITIL. Si vous effectuez une mise à niveau à partir d'un système non-ITIL, l'installation de CA SDM r12.9 effectue une mise à niveau vers un environnement ITIL.
- Si vous possédez une installation combinée de CA SDM r11.2 et de CA CMDB r11.1, vous ne pouvez pas effectuer de mise à niveau directe vers CA SDM r12.9. Vous *devez* tout d'abord mettre à niveau CA CMDB vers la version r11.2, puis exécuter la mise à niveau vers r12.9. Cette opération met à niveau CA SDM r11.2 vers r12.5, mais également CA CMDB r11.2 vers r12.5. Les versions CA CMDB r12.0 et r12.1 peuvent également être mises directement à niveau vers CA SDM r12.9.

  Remarque : Pour de plus amples renseignements sur la mise à niveau à partir d'une version antérieure, reportez-vous au *Manuel de mise en oeuvre de CA SDM r11.2.* Pour obtenir de l'aide et les correctifs de mise à niveau, contactez le soutien technique à l'adresse http://www.ca.com/worldwide.
- Avant d'effectuer la mise à niveau vers la version actuelle de CA SDM, vous devez comprendre les éléments suivants.
  - Remarques sur la base de données (page 31)
  - Conservation de vos personnalisations (page 35)
  - Remarques sur la migration LREL (page 40)
  - Remarques sur la transition d'état (page 41)
  - Remarques sur le courriel (page 42)
  - L'environnement linguistique UTF-8 doit être installé sur les plates-formes Linux/UNIX
- Sous Linux/UNIX, CA SDM n'utilise plus le script smtp_mail pour traiter les notifications de courriel sortantes. Si vous utilisez actuellement smtp_mail et que vous effectuez une mise à niveau vers la version actuelle, votre administrateur doit configurer les options de courriel appropriées à l'aide de la page Détail de la boîte aux lettres par défaut pour activer la fonctionnalité de notification de courriel de CA SDM.

Remarques sur la base de données

Avant de procéder à la mise à niveau vers CA SDM r12.9, tenez compte des renseignements suivants concernant la base de données :

- Sauvegardez votre base de données existante en suivant les procédures classiques de sauvegarde de base de données.
- (Applicable à tous les ordinateurs non Windows) Si votre version précédente de CA SDM est configurée avec une base de données Oracle 10gr2, installez le client Oracle 11gr2 avant d'effectuer une mise à niveau vers CA SDM r12.9.

  Important : Avant d'effectuer la mise à niveau, modifiez le chemin d'accès au répertoire de base Oracle afin d'utiliser le chemin d'accès au client oracle11g r2 dans le fichier $NXROOT/NX.env.
- Après la mise à niveau, aucune des versions (activées et désactivées) des KPI webLicenseCt n'est plus disponible et les données des KPI connexes ne sont plus valides. Ces données restent accessibles dans la table usp_kpi_data, mais elles ne sont plus extraites à des fins de signalement. Pour supprimer ces données, les clients peuvent exécuter la règle de l'indicateur clé de performance prédéfini ou bien les données des indicateurs clés de performance fournis par le système (désactivés par défaut).

  Important : Nous vous recommandons de vérifier les données disponibles dans la table usp_kpi_data, car l'exécution de cette règle KPI entraîne également l'archivage et/ou la purge les autres données de KPI collectées par le système.

  Remarque : Un nouveau KPI, webConcurrentTotalLicenseCt, est utilisé dans CA SDM r12.9 pour calculer le nombre d'utilisateurs uniques connectés à CA SDM pendant cet intervalle. Pour de plus amples renseignements, reportez-vous au *Manuel de mise en oeuvre*.
- Archivez le répertoire d'installation ($NX_ROOT) en suivant les procédures classiques d'archivage. Cette action réduit la quantité de données à déplacer et permet de gagner de l'espace disque.
- À partir d'une ligne de commande, exécutez le script approprié pour identifier les doublons d'enregistrements de votre base de données :

  Remarque : Exécutez ce script sur les serveurs secondaires. Si vous voulez exécuter ce script à l'aide de l'analyseur de requêtes SQL, modifiez le script SQLCHECK.SQL et supprimez l'argument de sortie avant d'exécuter la commande.

  - (Oracle) Exécutez OracleCheckr12UniqueIndexes.sql, situé dans le répertoire \Migrate du support d'installation.
  - (SQL Server) Ouvrez une fenêtre d'invite de commande et exécutez SQLCHECK.SQL comme suit :

    ```
    cd $NX_ROOT\samples\views\SQLServer
    ```

    Entrez la commande :

    ```
    Sqlcmd –E –e < SQLServer\SQLCHECK.SQL
    ```

Remarque : Après avoir effectué la mise à niveau vers CA SDM r12.9, vous trouverez ces fichiers dans *$NX_ROOT/samples/views/SQLServer* ou *$NX_ROOT/samples/views/Oracle* sur le serveur.

Important : Ces scripts identifient vos doublons d'enregistrements. Supprimez les doublons d'enregistrements identifiés avant d'effectuer la migration.

- Sous Windows, vous pouvez effectuer directement une mise à niveau à partir de r11.2, r12.0, r12.1, r12.5, r12.6 et r12.7
- Si vous avez installé CA SDM sous UNIX ou Linux, vous pouvez effectuer la mise à niveau à partir de r12.5, r12.6 et r12.7.
- Si votre installation contient une version antérieure du produit, par exemple CA SDM r11.2, r12.0, ou r12.1 dans une base de données ou un système d'exploitation UNIX/Linux non pris en charge, vous devez effectuer la mise à niveau vers CA SDM r12.5. Déplacez ensuite CA SDM vers un environnement d'exploitation et une base de données pris en charge avant d'effectuer la mise à niveau.
- Mettez à niveau votre système CA SDM r11.2 vers une base de données prise en charge (SQL Server et Oracle).

  Remarque : Pour de plus amples renseignements sur les bases de données prises en charge, reportez-vous aux *Notes de parution*.
- Effectuez une mise à niveau de Unicenter Service Desk r11.0 vers CA SDM r11.2 avant de migrer vos données vers une base de données prise en charge.
- Les caractères spéciaux de Windows, comme un long trait d'union, dans CA SDM ou Gestion des connaissances sur un système autre que Windows, ne sont pas stockés correctement dans la base de données.
- **Ingres** : si vous utilisez une base de données Ingres, convertissez vos données au format Oracle ou SQL Server avant d'effectuer la mise à niveau.

  Remarque : Pour de plus amples renseignements sur le processus de conversion, reportez-vous à la documentation de votre base de données.
- **Oracle** : Oracle ne prend pas en charge les index insensibles à la casse pour l'enregistrement de l'élément de configuration. Avant de démarrer la migration sur Oracle, vérifiez si SQLPlus et Oracle DB peuvent communiquer en utilisant le nom d'hôte. Si la communication échoue, vérifiez si Oracle est configuré avec l'adaptateur de bouclage.

  Remarque : Lorsque vous effectuez une migration dans un environnement de caractères codés sur deux octets avec une base de données Oracle, augmentez le nombre maximal de curseurs ouverts à au moins 500. Pour de plus amples renseignements, affichez les documents Oracle sur ORA-01000 (dépassement du curseur ouvert maximal).

- **SQL Server** : pour effectuer une mise à niveau de SQL Server vers la version actuelle de CA SDM, la base de données par défaut pour l'ID d'utilisateur de la base de données configuré doit être CA MDB. Si la base de données par défaut n'est pas CA MDB, la console de migration échouera et affichera le message suivant :

  "La MDB ne contient pas la table acctyp_v2."

- **Tomcat** (pour Unicenter Service Desk r11.0, r11.1 ou CA SDM r11.2) : si vous avez configuré Tomcat pour l'authentification externe, reconfigurez Tomcat manuellement pour l'authentification externe après la mise à niveau vers la version actuelle du produit.

- **Mises à jour de la table** : tenez compte des mises à jour suivantes qui ont lieu pendant la migration :

  - **Tables des états** : ces tables sont aussi mises à jour avec les enregistrements d'état appropriés lorsque les mêmes valeurs de code n'existent pas dans votre base de données. Par exemple, *Cr_Status* est mise à jour avec le code *AEUR* (En attente d'une réponse de l'utilisateur final).

  - **Domaines fonctionnels** : pour chaque rôle, la migration ajoute automatiquement une ligne pour chaque enregistrement *usp_functional_access*. La migration définit le niveau d'accès sur le même niveau pour chaque domaine fonctionnel de CA SDM r12.0 et r12.1 inclus dans la table *usp_role*. Les nouveaux domaines fonctionnels sont mappés en utilisant un champ de référence.

- **Clés étrangères** : tenez compte des renseignements suivants :

  - Les clés étrangères (SREL) désignant des tables, dont la clé principale est un UUID, passent du type entier au type UUID (ou 16 octets).

    Remarque : Pour de plus amples renseignements sur le paramétrage d'attributs SREL avec des valeurs de clé étrangère, reportez-vous au *Manuel de référence technique de CA SDM*.

  - Si vous avez supprimé des contraintes de clé étrangère dans votre ancien système CA SDM pour charger des données en série, recréez les contraintes de clé étrangère avant d'exécuter la mise à niveau. Les scripts qui suppriment les contraintes se trouvent aux emplacements suivants.

    - Oracle

      $NX_ROOT/samples/views/Oracle/OracleDropConstraints.sql

    - SQL Server

      $NX_ROOT/samples/views/SQLServer/SQLDropConstraints.sql

    Remarque : Pour réappliquer les contraintes supprimées, exécutez le script approprié : *OracleAddConstraints.sql* ou *SQLServer/SQLAddConstraints.sql*. Ces scripts se trouvent dans le même répertoire que les contraintes supprimées et contiennent des instructions dans les fichiers mentionnés.

- **MDB** : la MDB fournit un schéma de base de données cohérent pour diverses données de gestion des ressources informatiques. Pendant le développement de la MDB, les éléments de données de votre ancien environnement CA SDM ont été inclus dans ce schéma. La taille des éléments de données peut augmenter, ce qui accroît la taille globale de la base de données.

  Remarque : Lorsque les éléments de données standard s'étendent au-delà de la largeur de colonne définie pour la MDB, le processus de mise à jour peut tronquer des données dans ces éléments. Des messages vous indiquent toute troncature survenant lors de la mise à niveau.

- **Installation distribuée** : il est recommandé de mettre vos serveurs à niveau dans l'ordre ci-dessous, selon la configuration de CA SDM :

  - **Configuration conventionnelle**
    - Serveur principal
    - (Facultatif) Un ou plusieurs serveurs secondaires
  - **Disponibilité avancée**
    - Serveur d'arrière-plan
    - Un ou plusieurs serveurs de secours
    - Un ou plusieurs serveurs d'applications

- **Configuration d'une base de données distante** : tenez compte des renseignements suivants :

  Nous vous recommandons de mettre à niveau le serveur de base de données avec une nouvelle MDB avant de mettre à niveau le serveur principal. Si votre serveur de base de données est distant, exécutez l'installation de CA MDB sur le serveur de base de données avant d'exécuter la mise à niveau.

  - Si vous utilisez une base de données MDB SQL Server, sqlcmd doit se trouver sur l'ordinateur client avant la connexion à la MDB distante.

Remarques relatives à Gestion des connaissances

Avant d'effectuer la mise à niveau vers CA SDM r12.9, prenez en compte les renseignements Gestion des connaissances suivants pour vous aider dans cette opération :

- Les clients effectuant une mise à niveau à partir d'une version précédente de CA SDM qui utilisait le moteur de recherche FAST ESP *doivent* effectuer une migration vers le moteur de recherche EBR. La licence de FAST ESP expire en mai 2013. Pour passer au moteur de recherche EBR, cliquez sur Gestionnaire d'options, Moteur de recherche et modifiez ebr_version pour spécifier Moteur de recherche KT.
- Mise à niveau de Gestion des connaissances à partir de CA SDM r11.2 (page 78)
- Mise à niveau de Gestion des connaissances à partir de CA SDM r12.x (page 81)

Validation du type de document (DocType)

Les versions précédentes de CA SDM utilisaient le type de document suivant pour l'HTML généré à partir de formulaires HTMPL dans la propriété HtmplDoctype du fichier web.cfg :

```
HtmplDoctype <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
```

La propriété HtmplDoctype du fichier web.cfg s'affiche comme suit pour CA SDM r12.9 :

```
HtmplDoctype <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Frameset//EN"
"http://www.w3.org/TR/html4/frameset.dtd">
```

En règle générale, cette ligne commence dans la première liste d'une page.

Remarque : Après la mise à niveau vers CA SDM r12.9, vérifiez que la valeur de la propriété HtmplDoctype est modifiée dans vos formulaires personnalisés. Vous pouvez ouvrir un fichier HTML à partir du répertoire $NX_ROOT/bopcfg/www/wwwroot/html à l'aide de l'éditeur de texte pour vérifier la valeur de DocType.

Conservation de vos personnalisations

Avant d'effectuer la mise à niveau vers CA SDM r12.9, tenez compte des renseignements suivants concernant votre produit personnalisé :

Remarque : Lorsque vous fermez la console de migration avant la fin de la mise à niveau, le processus continue de s'exécuter en arrière-plan.

- **Rapports personnalisés** : lorsque vous personnalisez des rapports accédant à des tables de base de données de versions antérieures qui ont été déplacés vers des tables renommées, les noms de colonne sont modifiés dans r12.9.

  Remarque : Pour de plus amples renseignements sur les tables, reportez-vous au *Manuel de référence technique* de *CA SDM*.

- **Formulaires personnalisés :** la mise à niveau vers CA SDM r12.9 conserve les personnalisations des formulaires de la version précédente de CA SDM. Toutefois, vous ne pouvez pas afficher les fonctionnalités de CA SDM r12.9 dans les formulaires personnalisés après la mise à niveau.

- **Arborescence d'administration personnalisée** : si vous personnalisez l'arborescence d'administration dans Unicenter Service Desk r11.0, ces modifications ne seront pas mises à niveau en raison des modifications de l'architecture pour prendre en charge l'interface utilisateur basée sur les rôles. Ces personnalisations de l'arborescence d'administration incluent l'ajout de nouveaux noeuds, la modification du nom des noeuds existants, la modification des types d'accès ou d'autres données. Pour utiliser les personnalisations, procédez comme suit :

  1. Avant la mise à niveau, révisez votre arborescence d'administration Unicenter Service Desk r11.0 et notez les personnalisations que vous souhaitez utiliser après la mise à jour.
  2. À l'issue de la mise à jour, identifiez les rôles attribués aux personnalisations de l'arborescence d'administration.
  3. Appliquez les personnalisations à l'arborescence d'administration CA SDM r12.9 basée sur les rôles souhaitée.
  4. Effectuez des vérifications et des tests pour vous assurer que la fonctionnalité désirée a été conservée.

- **Boutons de formulaires personnalisés** : après la mise à niveau, les boutons des formulaires personnalisés dans */site/mods/htmpl* ne présentant pas de guillemets autour de la partie msgtxt(n) du code entraînent un message d'erreur, au lieu du nom du bouton.

  Par exemple, dans le formulaire detail_cr.htmpl, modifiez comme suit msgtxt(441) avec guillemets pour afficher le nom correct du bouton :

  ```
  ImgBtnCreate("btnchg", “msgtext(441)”, "detailSave('NEW_CHANGE')",
  true, 0, msgtext(440)); // Enregistrer et créer une demande de changement
  ```

- **Conservation des personnalisations** : si vous avez besoin des fonctions de CA SDM r12.9 et que vous souhaitez conserver vos personnalisations d'une version antérieure, vous devez réeffectuer les personnalisations dans un formulaire de base CA SDM r12.9, qui contient les fonctions r12.9.

  Remarque : lorsque vous personnalisez les rapports *acctypedtl.rpt* et *acctypesum.rpt*, les données renvoyées dans CA SDM r12.9 sont obsolètes.

- **Règles de notification** : lorsque vous supprimez les notifications d'activité par défaut Contact, Contacts d'objets et Types de contacts de l'installation antérieure de CA SDM, mais que vous souhaitez conserver cette fonction, notez les contacts par défaut supprimés avant la migration. Une fois la mise à niveau effectuée vers la nouvelle version, supprimez à nouveau les contacts de notification par défaut.

- **Fonctionnalité basée sur les rôles** : la mise à niveau peut causer des problèmes avec la fonctionnalité basée sur les rôles. Tenez compte des renseignements suivants.
  - Lorsque vous avez personnalisé l'un des formulaires suivants, ceux-ci sont considérés en lecture seule par l'Outil de conception Web dans CA SDM r12.9. Ils incluent une version xxx_site.htmpl dans laquelle vous pouvez utiliser du code personnalisé :
    - ahdtop.htmpl
    - menu_frames.htmpl
    - reports.htmpl
    - std_body.htmpl
    - std_footer.htmpl
    - std_head.htmpl
    - styles.htmpl
    - msg_cat.js
    - menu_frames_role.htmpl
- **Fichiers HTMPL personnalisés :** tenez compte des renseignements suivants :
  - Tous les fichiers HTMPL personnalisés conservent leurs paramètres de barre de menus par défaut après la mise à niveau. Une fenêtre contextuelle hérite de sa barre de menus à partir de l'onglet de la page principale, par l'entremise de l'interface utilisateur basée sur les rôles. Les fichiers HTMPL personnalisés ne sont pas disponibles dans les formulaires personnalisés de la version précédente après la mise à niveau.
  - CA SDM r12.9 n'utilise pas de fichier HTMPL personnalisé de versions précédentes. Le script de migration exécute le script perl $NX_ROOT/bin/*migrate_to_r12_9_web_check.pl*, qui ajoute les fichiers dotés de l'extension *incompatible_for_r2_9*. Une fois la migration terminée, ouvrez le fichier $NX_ROOT/site/web_check_files.txt à l'aide d'un éditeur de texte pour afficher la liste des formulaires incompatibles avec r12.9.
  - Si vous avez personnalisé le fichier list_dblocks.htmpl dans une version précédente de CA SDM, ce formulaire ne fonctionnera pas dans CA SDM r12.9. Si vous avez personnalisé l'arborescence d'administration pour afficher le fichier list_dblocks.htmpl à d'autres emplacements de l'arborescence, la personnalisation ne fonctionne pas après la migration. Modifiez le formulaire pour utiliser manuellement la nouvelle URL et le nouveau formulaire. Pour réaliser cette modification, cliquez sur Gestion des rôles et de la sécurité, Ressources de l'arborescence de menus et ouvrez Verrous actuels. Mettez à jour les ressources avec la chaîne de CA SDM r12.9 suivante :

    ```
    OP=SEARCH+FACTORY=record_lock+QBE.NN.lock_time=NULL
    ```

- **Clés étrangères** : lorsque le processus de mise à niveau détecte des problèmes d'intégrité référentielle lors de la tentative de réinitialisation des clés étrangères, des erreurs apparaissent dans le fichier migration.log. La clé étrangère associée est définie sur une référence valide prédéfinie.
- **Configuration des serveurs et du directeur Web** : lorsque votre précédente installation a été configurée pour utiliser des serveurs ou des directeurs Web supplémentaires, vous devez d'abord créer la configuration pour les serveurs spécifiques et exécuter l'utilitaire de configuration de serveurs CA SDM (pdm_configure). Pour de plus amples renseignements sur la création de configurations, consultez le Manuel d'administration.
- **Divisions de CA Automatisation du soutien** : lorsque vous migrez des divisions vers des clients hébergés, convertissez ces données avant d'activer et de configurer Automatisation du soutien dans CA SDM r12.9.

Renommage des formulaires HTMPL personnalisés

Si vous avez personnalisé des formulaires HTMPL dans une version précédente de CA SDM, avant d'effectuer la mise à niveau vers CA SDM r12.9, exécutez un script pour les renommer. Exécutez ce script sur tous les serveurs CA SDM. Le script migrate_to_r12_9_web_check.pl renomme tous les formulaires Web personnalisés, les feuilles de style, les scripts Java, les images et les macros du répertoire site/mods. Renommer ces fichiers permet d'identifier vos formulaires personnalisés.

1. Dans une invite de commande, exécutez pdm_perl $NX_ROOT/bin/migrate_to_r12_9_web_check.pl.

   Le script ajoute les formulaires personnalisés dotés d'une extension *incompatible_for_r12_9*.
2. Ouvrez $NX_ROOT/bin/migrate_to_r12_9_web_check.pl avec un éditeur de texte.

   Une liste de formulaires incompatibles avec r12.9 s'affiche.

Remarque : Le script ne restaure pas les fichiers des dossiers de sauvegarde dans les répertoires hérités ou site/mods comme dans les versions précédentes de CA SDM.

Renseignements supplémentaires :

Conservation de vos personnalisations (page 35)

Remarques concernant la migration de l'interface utilisateur

Avant de procéder à la mise à niveau vers CA SDM r12.9, tenez compte des informations suivantes relatives à la migration de l'interface d'utilisateur :

- La migration sauvegarde les formulaires automatiquement. Si vous utilisez des formulaires HTMPL personnalisés dans CA SDM r11.2, r12.0, r12.1 ou r12.5, vous *devrez* de nouveau les personnaliser après la mise à niveau vers CA SDM r12.9.
- Après la mise à niveau, modifiez tous les formulaires HTMPL personnalisés contenant des contrôles de carnet pour inclure les nouvelles macros Web et spécifier les noms de groupe d'onglets appropriés. Dans l'outil de conception Web, modifiez les instructions <PDM_NOTEBOOK> en <PDM_MACRO name=startNotebook> et les instructions <PDM_TAB> en <PDM_MACRO name=TAB>.

Option Web copy_inactive

Les nouvelles installations de CA SDM r12.9 n'incluent pas l'option Web copy_inactive dans le Gestionnaire d'options, de sorte que les liens aux objets désactivés ne soient pas copiés. Si vous effectuez une mise à niveau à partir de CA SDM r12.5 ou r12.6, les liens aux objets désactivés seront copiés, car la migration effectue l'installation de l'option.

Si vous n'installez pas l'option copy_inactive, tenez compte des informations suivantes :

- CA SDM ne copie pas les SREL qui pointent vers des objets désactivés, excepté si SREL est requis.

  Par exemple, l'organisation org1 possède un emplacement désactivé. Lorsque vous copiez org1, la nouvelle organisation ne possède aucun emplacement. Toutefois, si SREL est requis, CA SDM ignore cette règle et copie l'emplacement. Par exemple, CA SDM ignore la règle et vous pouvez copier un CI contenant une classe inactive.
- CA SDM ne copie pas les relations LREL (plusieurs à plusieurs) vers des objets désactivés.

  Par exemple, le CI appelé CITest1 dispose d'une relation avec l'organisation inactive org2. Lorsque vous copiez CITest1, org2 n'est pas associée au nouveau CI.

Important : Ces règles s'appliquent également lorsque vous copiez un ticket, même s'il est créé à partir d'un modèle. Si vous avez installé copy_inactive, l'exception à la règle concerne les zones inactives et les catégories, qui ne sont pas copiées à partir de tickets existants ni remplies à partir de modèles.

Remarques sur la migration LREL

Une *relation de liste* (LREL) représente une association entre deux objets. Une LREL a une relation côté gauche (lhs) et côté droit (rhs). Chaque côté de la relation est un attribut de l'objet majic qui contient la relation de données.

Dans les versions précédentes du produit, les instructions et .maj LREL et les objets décrivaient des relations plusieurs-à-plusieurs entre les données du SGBD. Les relations de type plusieurs-à-plusieurs n'utilisent plus l'instruction LREL majic. A la place, les tables individuelles stockent les deux côtés de la relation. Les objets accèdent à la relation avec une instruction BREL standard. Par exemple, vous pouvez voir la relation entre les demandes de changement et les CI en examinant la nouvelle table usp_lrel_asset_chgnr et l'objet lrel_asset_chgnr correspondant.

Les modifications de LREL rendent inutile le stockage des noms d'attribut dans la base de données. Les deux côtés de la relation sont des relations de clés étrangères uniques (SREL) qui sont faciles à joindre et à indexer. Si nécessaire, la relation peut contenir des attributs relationnels supplémentaires.

Pendant la mise à niveau, les activités suivantes se produisent quand les données de la table LREL migrent vers r12.9 :

- Le système fait automatiquement migrer les tables et les objets avec des relations LREL vers les tables et les objets r12.9.
- Le système nomme les nouvelles tables en utilisant le format *usp_lrel_lhsName_rhsName*.

  Par exemple, la table *usp_lrel_asset_chgnr* a une relation à gauche avec les actifs et à droite avec les demandes de changement.
- Le système nomme les objets correspondants en utilisant *lrel_lhsName_rhsName*.

  Par exemple, l'objet *lrel_asset_chgnr* correspond à la table *usp_lrel_asset_chgnr*.
- A cause d'une restriction de base de données, certains noms sont abrégés.
- Vos données migrent des anciennes tables vers les tables r12.9 et tout le code de CA SDM est modifié pour utiliser ces tables.
- Le système n'utilise plus les anciennes tables de base de données LREL, comme *bmlrel*. Cependant, les anciennes tables conservent les données à des fins de référence.
- Un attribut de relation inverse (BREL) vers le nouvel objet remplace l'attribut LREL d'origine dans chaque définition d'objet majic liée.
- Si vous utilisez une API prise en charge, comme la méthode de service Web *CreateLrelRelationship()*, le code fonctionne comme prévu.

- Si vous avez ajouté des relations personnalisées de style LREL, CA SDM les fait migrer vers des tables r12.9.
- Les codes définis par site ou les rapports qui accèdent directement aux anciennes tables LREL utilisent d'anciennes données car le système n'utilise plus ces tables. Nous vous conseillons de mettre à jour le code afin d'utiliser les tables r12.9 pour que le code et les rapports s'exécutent correctement.

Important : Si votre code accède directement à des objets ou à des tables LREL hérités, le code va échouer après la migration. Nous vous conseillons de mettre le code à niveau avant de procéder à la migration. Par exemple, si votre code utilise des instructions majic pour établir des relations LREL, utilisez la méthode *createLrelRelationships()* au lieu de remplir directement une table.

Remarque : Il est recommandé de vérifier le code défini par le site ou les rapports qui accèdent directement à la base de données, ou qui adressent les objets majic LREL hérités (comme l'objet lrel1) pour vous assurer qu'ils fonctionnent correctement. Vous pouvez mettre votre code à jour pour qu'il utilise une interface prise en charge, par exemple les services Web. Vous pouvez également mettre à jour les noms des tables nécessaires. En ce qui concerne les rapports, vous pouvez également actualiser les requêtes avec les nouvelles références de la table du SGBD.

Remarques sur la transition d'état

Si vous prévoyez d'utiliser des transitions d'état après la mise à niveau à partir de CA SDM r11.2, r12.1 et r12.1 vers CA SDM r12.9, tenez compte des informations suivantes :

- Les transitions d'état sont désactivées lorsque vous effectuez une mise à niveau vers r12.9.

  Remarque: Toutes les descriptions de codes d'état personnalisés qui apparaissent dans des formulaires de ticket sont conservées pendant le processus de mise à niveau.
- Par défaut, l'option *Status_Policy_Violations* est installée et définie sur Avertissement après la mise à niveau. Ce paramètre autorise les transitions non définies mais consigne un avertissement.
- Si vous définissiez cette option sur Autoriser, les transactions non définies ne sont pas consignées.

  Remarque : Pour plus d'informations sur l'option *Status_Policy_Violations*, reportez-vous à *l'Aide en ligne*.

Mise à niveau de la messagerie

CA SDM remplace les options de messagerie entrante du gestionnaire d'options par une boîte aux lettres (table *usp_mailbox*) qui fournit des options correspondantes. Les options de messagerie sortante existent toujours dans le gestionnaire d'options. Lorsque vous effectuez une mise à niveau, CA SDM utilise vos paramètres de courriel existants pour configurer une boîte aux lettres au lieu d'utiliser les paramètres de Boîte aux Lettres par défaut fournis avec CA SDM r12.9. Chaque option de messagerie, sauf EMAIL_ATTACHMENT_DIR (qui est désormais inutile), est mappée à une option de la table *usp_mailbox*. Une option qui n'est pas définie est définie comme étant nulle dans la table.

Remarque : Pour plus d'informations sur l'activation de la boîte aux lettres par défaut et sur l'utilisation des options de la boîte aux lettres, reportez-vous au *Manuel d'administration* et à *l'Aide en ligne*.

Le tableau suivant répertorie les options supprimées des options de messagerie, fournies dans la table *usp_mailbox*, et précise leurs étiquettes dans la page Détails de la boîte aux lettres.

Option de messagerie	Option usp_mailbox	Etiquette dans les détails de la boîte aux lettres par défaut
EMAIL_ALLOW_ANONYMOUS	allow_anonymous	Autoriser les contacts anonymes
EMAIL_ATTACHMENT_DIR	N/D	N/D **Remarque :** Etant donné que l'utilisation de EMAIL_ATTACHMENT_DIR est désapprouvée, vous devez sélectionner manuellement un référentiel de pièces jointes si cette option était définie et que EMAIL_ATTACHMENT_REPOSITORY ne l'était pas.
EMAIL_ATTACHMENT_ REPOSITORY	attmnt_repository	Référentiel des pièces jointes
EMAIL_FORCE_ATTACHMENT_ SPLITOUT	split_out_attachment	Forcer le fractionnement de la pièce jointe
EMAIL_IS_ATTACHMENT	attach_email	Joindre le courriel complet
EMAIL_SAVE_UNKNOWN_ EMAILS	save_unknown_emails	Enregistrer les courriels inconnus
MAIL_EATER_IMAP_HOST_PORT	host_port	Remplacement du port
MAILEATER_CHECK_MAIL_ INTERVAL	check_interval	Intervalle de vérification
MAILEATER_HOST	host_name	Nom d'hôte

Option de messagerie	Option usp_mailbox	Etiquette dans les détails de la boîte aux lettres par défaut
MAILEATER_LOGIN_PASSWORD	mot de passe	Mot de passe
MAILEATER_LOGIN_USERID	userid	ID d'utilisateur
MAILEATER_POP3_HOST_PORT	host_port	Remplacement du port
MAILEATER_SECURITY_LEVEL	security_lvl	Niveau de sécurité
MAILEATER_SERVER_TYPE	email_type	Type de courriel :

Important : Le paramètre Répertoire des pièces jointes est désapprouvé dans r12.9. Vous *devez* donc spécifier un référentiel de pièces jointes avant de continuer à interroger les boîtes aux lettres.

Remarques sur Maileater.cfg

Des informations précédemment incluses dans le fichier *maileater.cfg* sont désormais mappées vers la table *usp_mailbox_rule* dans r12.9. Tenez compte des informations suivantes sur le mappage de *maileater.cfg* à *usp_mailbox_rule* :

- Le -i au début de la ligne indique la non-distinction majuscules/minuscules et établit un mappage vers le champ filter_ignore_case.
- Le filtre de recherche Objet : *... désignait précédemment une expression régulière utilisée pour le filtrage. Le filtre Objet : est supprimé. Il est remplacé par un symbole ^ et la valeur restante est mappée vers le champ *filter_string*. Le Filter_type est défini sur le type Contenu du sujet.
- TEXT_API xxx identifie l'objet qui est traité pour une règle. La chaîne TEXT_API a été supprimée et ce qui reste est mappé vers le champ *action_object*. Le champ *action_operation* est défini sur Créer/Mettre à jour un objet.
- La réponse à l'utilisateur contient généralement PDM_MAIL …. Si PDM_MAIL est défini, définissez reply_method sur 1800 ou laissez cette valeur nulle.
- Si le paramètre -s est défini, supprimez le champ d'objet du texte et définissez *reply_subject* avec cette valeur.
- Cette fonctionnalité conserve l'ordre des entrées. Un numéro séquentiel commençant à 100 et augmentant par incréments de 100 est défini pour chaque ligne valide.

Les autres champs de *usp_mailbox_rule* sont définis comme suit :

Champ	Valeur
boîte aux lettres	Par défaut
action_write_to_log	0

Champ	Valeur
action_log_prefix	null
delete_flag	0
description	Migré depuis le fichier pdm_maileater.cfg
reply_failure_html	<ne pas renseigner pour hériter de l'action par défaut>
reply_failure_text	<ne pas renseigner pour hériter de l'action par défaut>
reply_success_html	<ne pas renseigner pour hériter de l'action par défaut>
reply_success_text	<ne pas renseigner pour hériter de l'action par défaut>
text_api_defaults	null
text_api_ignore_incoming	null
action_subject_handling	null
last_mod_dt	null
last_mod_by	null
inclusion_list	"*"
email_address_per_hour	-1
exclusion_list	null
log_policy_violation	1

Fonctionnement de la console Web

La console de migration vous guide dans la migration et les processus de mise à niveau pour CA SDM. La console détecte automatiquement une installation existante, comme CA SDM r11.2. Vous pouvez démarrer la mise à niveau à partir du support d'installation ou la démarrer manuellement (page 45).

Remarque : Si vos formulaires Web personnalisés ne sont pas compatibles avec CA SDM r12.9, la console de migration affiche un message indiquant que ces formulaires ont été déplacés vers le répertoire site/mods/wwww/htmpl. Pour de plus amples renseignements sur ces formulaires, consultez le fichier Web_Forms_Changed.txt dans le répertoire site/mods/.

Important : La console de migration de CA SDM ne convertit pas les divisions vers des clients hébergés. Si vous voulez configurer Automatisation du soutien dans un environnement d'hébergement multiclient, vous *devez* migrer séparément (page 52) les divisions CA Automatisation du soutien r6.0 SR1 eFix5 vers des clients hébergés CA SDM r12.9 avant d'activer Automatisation du soutien dans CA SDM.

Le moteur accomplit les tâches suivantes :

1. Vérifie que la version de votre produit est CA SDM r11.2, r12.0, r12.1, r12.5, r12.6 ou r12.7.
2. Convertit les mots de passe en un format conforme à la norme FIPS 140-2.
3. Applique les mises à jour de la MDB.

   Important : La version MDB distante doit au moins être CA MDB r1.5. Sinon, la migration échoue.
4. Migre les données LREL.
5. Convertit les fichiers personnalisés en UTF-8.
6. Convertit les enregistrements de type d'accès en enregistrements de type d'accès et de rôle <UDSK> r12.9.
7. Migre et met à niveau les demandes de tableau de résultats d'utilisateur pour les opérations basées sur les rôles.
8. Migre et met à niveau les notifications existantes pour utiliser des règles de notification et des modèles de message de notification.

Remarque : Après avoir sélectionné Mettre à niveau et cliqué sur Installer, vous ne pouvez pas annuler la migration ni la mise à niveau. Si vous fermez la console de migration avant la fin de la mise à niveau, le processus continue à s'exécuter en arrière-plan.

Fichier journal de migration

Si vous rencontrez des problèmes pendant la migration et la mise à niveau, le journal de migration fournit un enregistrement de l'ensemble du processus. Vous pouvez accéder à ce journal à l'emplacement suivant :

```
$NX_ROOT/log/pdm_migrationr12_9.log
```

Démarrez la migration manuellement.

Vous pouvez démarrer manuellement la mise à niveau à l'aide de la commande suivante :

- **Windows**

  ```
  $NX_ROOT\bin\migrate_to_r12_9.vbs
  ```
- **Linux/UNIX**

  ```
  $NX_ROOT\bin\migrate_to_r12_9.sh
  ```

Remarque : Si la migration échoue en raison d'une erreur de "validation du schéma", utilisez la commande mentionnée plus haut pour réexécuter la mise à niveau.

Mise à niveau de CA CMDB à partir d'une version antérieure

Vous pouvez mettre CA CMDB à niveau vers CA SDM r12.9 à partir d'une version antérieure, par exemple r11.2, r12.0 ou r12.1. Si vous annulez la migration, vous *devez* exécuter le script pour relancer la console de migration. Le script se trouve dans le répertoire */bin* du produit, par exemple *C:/CMDB/bin*. Par exemple, pour annuler une migration sous Linux ou UNIX, exécutez le script *migration_to_r12.9.sh*.

Remarque : Si vous mettez à niveau une version autonome de CA CMDB, vous pouvez continuer à utiliser la fonction autonome CA CMDB dans CA SDM r12.9. Si vous effectuez la mise à niveau à partir d'un environnement incluant CA CMDB et CA SDM, ou si la mise à niveau s'effectue à partir d'un environnement CA SDM dépourvu de CA CMDB, l'ensemble de CA SDM r12.9 est installé lors de la mise à niveau.

La mise à niveau de CA CMDB s'effectue comme suit :

1. Lancez le programme d'installation de CA SDM à partir du support d'installation.

   Le programme d'installation détecte votre version du produit, par exemple CA CMDB r11.2.

   Remarque : Si vous effectuez la mise à niveau à partir d'une installation associant CA SDM et CA CMDB, le programme d'installation affiche l'environnement détecté comme une version de CA CMDB et non de CA SDM.

2. Cliquez sur Suivant.

   L'installation vous avertit de ne pas utiliser CA SDM et Gestion des connaissances tant que la migration n'est pas terminée.

3. Cliquez sur Suivant.

   Si l'installation détecte le visualiseur, vous êtes invité à le désinstaller manuellement.

   Important : Après avoir désinstallé le visualiseur, vous *devez* redémarrer et relancer le programme d'installation de CA SDM.

4. Acceptez les termes du contrat de licence et cliquez sur Installer.

   L'installation sauvegarde vos données et arrête les services.

   Remarque : La mise à niveau de CA CMDB n'effectue *pas* de sauvegarde de votre base de données.

   Une fois l'installation terminée, la console de migration affiche un avertissement vous invitant à consulter la documentation relative à la migration.

5. Cliquez sur Migrer.

   La console de migration charge des données système, met à jour votre MDB et redémarre des services.

   Remarque : Vous pouvez afficher le journal de migration de façon active pendant le processus.

6. La console vérifie des tables, traite les données, effectue une sauvegarde et met votre produit à niveau vers r12.9.

   La boîte de dialogue de configuration de CA SDM s'affiche.

7. (Facultatif) Configurer uniquement CA CMDB.

   Si vous effectuez une mise à niveau à partir d'un environnement CA CMDB autonome, une case à cocher *Configurer uniquement CA CMDB* apparaît sur le formulaire Paramètres généraux.

   Important : Pendant la configuration, lorsque vous migrez de la version autonome de CA CMDB vers CA SDM, une case à cocher Configurer uniquement CA CMDB s'affiche. Lorsque vous désactivez la case à cocher Configurer uniquement CA CMDB et que vous cliquez sur Suivant, vous ne pouvez pas configurer CA CMDB à nouveau. Même si vous cliquez sur Retour, la case à cocher Configurer uniquement CA CMD n'est plus disponible. Un message vous avertit de ce comportement dans la boîte de dialogue de configuration. Si vous annulez la configuration avant la fin et la reprenez, la case à cocher Configurer uniquement CA CMD est disponible.

   La case à cocher Configurer uniquement CA CMD contrôle la valeur de la variable d'environnement CA SDM NX_CMDB. La variable d'environnement contrôle si la fonctionnalité Automatisation du soutien est configurée. Si la case à cocher est désactivée, la fonctionnalité Automatisation du soutien est configurable, sinon il ne l'est pas. La variable d'environnement affecte le comportement de certains formulaires Web.

   Si vous effectuez une mise à niveau à partir d'un environnement CA CMDB autonome et que vous souhaitez utiliser la fonctionnalité CA CMDB autonome dans CA SDM r12.9, vous ne pouvez pas configurer l'Automatisation du soutien.

8. Terminez la configuration comme il convient pour votre environnement.

Migration de CA SDM r12.9 sur un système d'exploitation Linux/UNIX 64 bits

Remarque : Ces renseignements s'appliquent aux systèmes Linux/UNIX 64 bits uniquement.

1. Installez le client Oracle 32 bits.
2. Connectez-vous à Oracle_Server_SID.
3. Créez un nom de service Net local et testez la connexion.
4. Exportez la variable TWO_TASK.
5. Modifiez les variables ORACLE_HOME et PATH pour obtenir le chemin d'accès au répertoire de base de oracle_client et supprimez le chemin d'accès au répertoire de base du serveur, comme illustré dans l'exemple suivant :

   ```
   ORACLE_HOME= /opt/app/product/11.2.0/client_1
   PATH= /opt/app/product/11.2.0/client_1/bin
   ```

   Remarque : Mettez à jour la variable ORACLE_HOME dans NX.env comme indiqué dans l'exemple précédent.
6. Définissez LD_LIBRARY_PATH et LIBPATH dans les fichiers binaires 32 bits de la bibliothèque du client, comme illustré dans l'exemple suivant :

   ```
   LD_LIBRARY_PATH=/opt/app/product/11.2.0/client_1/lib
   ```
7. Exécutez pdm_configure avec ORACLE_HOME défini sur client_home, comme illustré dans l'exemple suivant :

   C:\app\Administrator\product\11.2.0\client_1\
8. Installez CA SDM r12.9.

Migration de CA SDM r12.9 sur un système d'exploitation Windows 64 bits

Remarque : Ces informations s'appliquent aux systèmes Windows 64 bits uniquement.

Pour migrer des données vers CA SDM r12.9, procédez comme suit :

1. Installez le client Oracle 32 bits.
2. Connectez-vous à Oracle_Server_SID.
3. Créez un nom de service Net local et testez la connexion.
4. Modifiez la variable PATH pour obtenir le chemin d'accès au répertoire de base de oracle_client et supprimez le chemin d'accès au répertoire de base du serveur, comme illustré dans l'exemple suivant :

   C:\app\Administrator\product\11.2.0\client_1\bin
5. Exécutez pdm_configure avec ORACLE_HOME défini sur client_home, comme illustré dans l'exemple suivant :

   C:\app\Administrator\product\11.2.0\client_1\
6. Installez CA SDM r12.9.

Exemple : Migration d'un environnement Windows non pris en charge

Dans cet exemple, CA SDM r11.2 est installé sous Windows 2003 (32 bits) avec SQL Server 2005. Vous voulez effectuer une migration de vos données et une mise à niveau vers CA SDM r12.9 sur un système Windows 2008 64 bits avec SQL Server 2008.

1. Effectuez la migration vers CA SDM r12.9 sur le même ordinateur.
2. Effectuez la mise à niveau de SQL Server 2005 vers la version 2008.
3. Sauvegardez la base de données MDB.
4. Installez CA SDM r12.9 sur Windows 2008 (64 bits).
5. Chargez la sauvegarde de la MDB réalisée à l'étape 3.
6. Déplacez le dossier $NX_ROOT\site\mod de l'ordinateur ancien vers le nouvel ordinateur.
7. Mettez à jour le fichier NX.env avec les variables personnalisées.
8. Copiez le dossier de pièces jointes de l'ordinateur ancien vers le nouvel ordinateur.

9. Exécutez à nouveau la configuration sur le nouvel ordinateur.
10. Mettez à jour les détails de l'ordinateur aux emplacements requis dans le Gestionnaire d'options.

Exemple : Migration d'un environnement non-Windows non pris en charge

Dans cet exemple, r11.2 CA SDM est installé sous Redhat Enterprise Linux 4 avec Oracle 10g. Vous voulez effectuez la migration de vos données et la mise à niveau vers CA SDM r12.9 sous un système Redhat Enterprise Linux 6 avec Oracle 11g R2.

1. Effectuez la migration vers CA SDM r12.5 sur le même ordinateur.
2. Sauvegardez la base de données MDB.
3. Installez CA SDM r12.5 sous Redhat Enterprise Linux 6 avec Oracle 11g R2.
4. Chargez la sauvegarde de la MDB réalisée à l'étape 2.
5. Déplacez le dossier $NX_ROOT\site\mod de l'ordinateur ancien vers le nouvel ordinateur.
6. Mettez à jour le fichier NX.env avec les variables personnalisées.
7. Copiez le dossier de pièces jointes de l'ordinateur ancien vers le nouvel ordinateur.
8. Exécutez à nouveau la configuration sur le nouvel ordinateur.
9. Mettez à jour les détails de l'ordinateur aux emplacements requis dans le Gestionnaire d'options.
10. Effectuez la migration à partir de CA SDM r12.5 vers r12.9.

Migration de données Automatisation du soutien

Vous pouvez faire migrer des données CA Automatisation du soutien r6.0 SR1 eFix5 vers CA SDM r12.9 depuis les environnements suivants :

- Unicenter Service Desk r11.2
- CA SDM r12,0
- CA SDM r12,1
- CA Automatisation du soutien r6.0 SR1 eFix5 sans CA SDM.

Remarque : Vous pouvez uniquement migrer des données de CA Automatisation du soutien r6.0 SR1 eFix5. Nous vous conseillons d'exécuter une sauvegarde complète de votre base de données CA Automatisation du soutien r6.0 SR1 eFix5 avant de procéder à la migration.

Important : La stratégie de marque de CA Automatisation du soutien r6.0 SR1 eFix5 ne migre pas automatiquement vers CA SDM r12.9. Il est recommandé d'examiner la stratégie de marque personnalisée afin de vérifier qu'elle correspond à celle de CA SDM. Si nécessaire, copiez et collez l'en-tête, le pied de page et les données de l'URL CSS de chaque division vers le client hébergé correspondant (ou public) dans CA SDM pour migrer les données de stratégie de marque.

Migration d'une base de données Automatisation du soutien

Vous pouvez configurer l'outil de migration pour faire migrer des données de la base de données Automatisation du soutien vers la base de données CA SDM, y compris les transformations de noms Automatisation du soutien dans les conventions de la base de données USDK>. Procédez à la migration des données de la base de données Automatisation du soutien vers la base de données CA SDM avant la première utilisation de Automatisation du soutien.

Le processus ci-dessous explique le mode de migration des données.

1. Exportez (page 53) les données CA Automatisation du soutien à l'aide du script se trouvant sur le support d'installation.

   L'outil d'exportation convertit les données au format *.DAT.* Lorsque vous procédez à la migration, l'outil effectue les opérations importantes suivantes :

   - Il importe le schéma de base de données Automatisation du soutien dans la base de données CA SDM.

     Ce schéma crée les tables nécessaires que Automatisation du soutien utilise.

- Il fait migrer les données XLM de la migration de la base de données Automatisation du soutien vers la base de données CA SDM.

  L'outil de migration de CA SDM génère les UUID nécessaires et crée les enregistrements requis qui représentent des relations entre l'ID de Automatisation du soutien et l'UUID de CA SDM.

2. Copiez le dossier d'exportation des données Automatisation du soutien de CA vers le répertoire suivant sur le serveur de CA SDM :

   NX_ROOT/site/sbmigration/SA60

   L'exportation des données est terminée.

3. Importez (page 55) les données dans CA SDM en utilisant l'outil de migration CA Automatisation du soutien.

   Les données se chargent dans la base de données et la migration est terminée

Migration de données historiques

Si vous ne voulez pas faire migrer toutes les données historiques de la base de données CA Automatisation du soutien r6.0 SR1 eFix5, vous pouvez supprimer quelques-unes de ces données historiques. Vous pouvez configurer le nombre de jours à conserver dans la base de données dans la configuration du script de purge.

Le script de purge est disponible au téléchargement sur le site :

ftp://ftp.ca.com/pub/supportbridge/6,0/patch-01/purge_history_6,0_sp1.zip

Procédure de conversion des divisions à des clients hébergés

Vous pouvez uniquement migrer les divisions de CA Automatisation du soutien r6,0 SR1 eFix5. Vous convertissez ces divisions en clients hébergés pour utiliser l'hébergement multiclient dans un environnement Automatisation du soutien. Vous pouvez faire migrer chaque division séparément comme son propre client hébergé. Pendant l'importation initiale des données, toutes les lignes des tables avec client hébergé facultatif ont un client hébergé.

Important : Vous devez migrer ces données avant d'activer Automatisation du soutien dans CA SDM.

Vous pouvez faire migrer des divisions vers des clients hébergés de la façon suivante :

1. Exportez (page 53) les données de division à l'aide du script figurant sur le support d'installation.

   Vous pouvez exporter une seule division ou toutes les divisions.

2. L'outil d'exportation convertit les données au format *.DAT.*

   L'outil affiche l'état de l'exportation de la division.

3. Copiez le dossier d'exportation des données Automatisation du soutien de CA vers le répertoire suivant sur le serveur de CA SDM :

   NX_ROOT/site/sbmigration/SA60

   L'exportation des données est terminée.

4. Importez (page 55) les données dans CA SDM en utilisant l'outil de migration CA Automatisation du soutien.

   Les données se chargent dans la base de données et la migration est terminée

Remarque : Pour plus d'informations sur la configuration de Automatisation du soutien, reportez-vous à l'*Aide en ligne*.

Exportation des données Automatisation du soutien de CA

Pour exporter des données CA Automatisation du soutien r6.0 SR1 eFix5, convertissez-les au format *.DAT* utilisé par CA SDM. Vous pouvez exporter des divisions dans des clients hébergés indépendants et importer les données dans un environnement public. L'outil d'exportation consigne le processus et affiche le répertoire de sortie du fichier journal une fois l'exportation terminée. Le processus d'exportation enregistre la sortie réussie de chaque table et indique toute condition ou erreur inattendue qu'il a rencontrée.

Important : Vous pouvez uniquement migrer les divisions de CA Automatisation du soutien r6,0 SR1 eFix5.

Pour exporter des données CA Automatisation du soutien

1. Exécutez le script *SA60Export* se trouvant sur le support d'installation dans le répertoire suivant :

   /casd.nt/SAMigration.

   Remarque: L'extension de fichier dépend de votre système d'exploitation. Par exemple, Windows utilise bat, UNIX utilise sh pour le script interpréteur Bourne, csh pour l'interpréteur C ou ksh pour l'interpréteur Korn, etc.

   L'outil de migration de CA Automatisation du soutien apparaît.

2. Procédez de la manière suivante :

   a. Entrez le répertoire parent WEB-INF pour l'installation de CA Automatisation du soutien r6.0 SR1 eFix5.

   b. Entrez un répertoire vers lequel exporter vos données CA Automatisation du soutien.

      Remarque : Une fois l'exportation terminée, déplacez ce dossier vers le répertoire *NX_ROOT/site/sbmigration/SA60* sur le serveur CA SDM.

c. (Facultatif) Spécifiez si les mots de passe peuvent être exportés. Si vous sélectionnez cette option, les mots de passe sont exportés pour les utilisateurs, les informations d'identification par défaut et les informations d'identification de tâche automatisée.

d. (Facultatif) Exportez une seule division ou toutes les divisions. Si vous sélectionnez cette option, une liste déroulant affiche toutes les divisions actives.

3. Cliquez sur Run (Exécuter).

   L'état du processus affiche des informations sur l'exportation (par exemple, la table de base de données qui migre) et le nombre d'enregistrements dans la table.

   Un message apparaît si l'outil détecte des erreurs irrécupérables.

   Remarque : Vous pouvez arrêter l'exportation en sélectionnant Arrêter dans la barre d'outils ou dans le menu Fichier.

   L'exportation des données est terminée.

4. Configurez et mettez en oeuvre Automatisation du soutien d'une façon adaptée à votre environnement.

   Remarque : Pour plus d'informations sur la configuration des options de Automatisation du soutien, reportez-vous à l'*Aide en ligne*.

Importation de données Automatisation du soutien

Les données Automatisation du soutien sont importées après avoir été converties au format *.DAT*. Vous pouvez importer des données dans CA SDM utilisant le script de migration de Automatisation du soutien. Vous appelez l'utilitaire après avoir installé et configuré CA SDM. Vous pouvez aussi exécuter *sa_migrate.pl* à l'aide de la commande *pdm_perl*.

Vous pouvez accéder au script dans le répertoire *NX_ROOT\bin*. Le script de migration effectue des tâches telles que le traitement des tables pour respecter les contraintes de base de données, la création des objets CA SDM correspondants, le mappage des valeurs de colonnes des clients hébergés, etc.

L'emplacement par défaut des fichiers en rapport avec la migration dans l'installation de CA SDM est le répertoire *NX_ROOT/site/sbmigration*. Le fichier de configuration de l'importation, par exemple, se trouve dans le dossier *NX_ROOT/site/sbmigration/config*. Le fichier *sa_migration_config.dat* stocke les colonnes id, prop_name, value et prop_description au format de données de CA SDM.

Le répertoire stocke les données d'exportation de CA Automatisation du soutien r6.0 SR1 eFix5, le code de l'utilitaire de migration, les scripts Perl, etc.

Pour importer des données Automatisation du soutien

1. Démarrez le service CA SDM.

   Le service démarre et vous pouvez vérifier qu'il s'exécute.

2. Entrez la commande ci-dessous dans la ligne de commande :

   ```
   pdm_perl <NX_ROOT>\bin\sa_migrate.pl
   ```

   Les données Automatisation du soutien se chargent dans la base de données depuis la trousse d'exportation.

Configuration de l'accès aux rôles de Automatisation du soutien après la migration

Si vous configurez Automatisation du soutien avant la migration, l'accès aux rôles est correctement configuré. Si vous configurez Automatisation du soutien après la migration, définissez la valeur appropriée pour chaque champ d'accès à Automatisation du soutien. Si l'accès aux rôles n'est pas correctement configuré, vous ne pouvez pas accéder à l'interface analyste ou à l'interface utilisateur final de Automatisation du soutien.

Le processus suivant explique comment configurer l'accès aux rôles de Automatisation du soutien après la migration :

1. Installez l'option *supportautomation_url*.

2. Définissez le champ d'accès à Automatisation du soutien pour chaque rôle que vous voulez autoriser à accéder à Automatisation du soutien.

Remarque : Pour plus d'informations sur l'installation de l'option *supportautomation_url* ou la création de rôles d'accès à Automatisation du soutien, consultez *l'Aide en ligne*.

Migration d'un univers CA Business Intelligence personnalisé

La migration d'un univers personnalisé s'effectue de la façon suivante.

1. Suivez les instructions de personnalisation pour lier un univers personnalisé vers l'univers CA SDM.
2. Sauvegardez le fichier *.biar* de tous les univers ou rapports définis par le site.
3. Installez un univers provenant d'une version actuelle.
4. Reliez l'univers personnalisé à l'univers provenant de la version actuelle.

Sauvegarde d'un univers personnalisé

Si vous avez lié un univers personnalisé à l'univers CA SDM, exécutez les actions suivantes avant d'installer l'univers et les rapports CA SDM r12.9.

1. Utilisez l'assistant d'importation pour créer un fichier *.biar* de sauvegarde des univers ou rapports définis par le site.
2. Démarrez Universe Designer.
3. Importez votre univers personnalisé.
4. Enregistrez une copie de l'univers sur votre lecteur local.

   L'univers personnalisé est sauvegardé.

Informations complémentaires :

Déplacement du développement à la production (page 515)

Installation d'un univers CA Business Intelligence

Vous installez l'univers pour remplacer l'univers et les rapports de CA Business Intelligence version12.0.

Pour installer l'univers

1. A partir du DVD 2 de CA Service Desk Manager, exécutez le fichier setup.exe.
2. Cliquez sur l'onglet Installation de produits.
3. Faites défiler la liste et sélectionnez Configuration de CA Business Intelligence.

   L'assistant d'installation des composants de CA Service Desk Manager s'affiche.
4. Cliquez sur Suivant et entrez vos informations d'identification.

   Remarque : Si CA SDM n'est pas installé sur cet ordinateur, spécifiez le nom d'hôte CA SDM.
5. Cliquez sur Terminer.

   L'univers et les rapports CA Business Intelligence version12.0 sont remplacés et les rapports r12.9 sont créés dans les sous-dossiers.

Mise à jour d'un lien d'univers

Bien que le nom d'univers reste inchangé dans CA SDM r12.9, vous *devez* mettre à jour le lien d'univers vers l'univers. Sinon, vous pouvez rencontrer des problèmes de connexion à l'univers lorsque vous exécutez vos rapports et lorsque vous importez l'univers. Le message d'erreur suivant peut survenir.

Impossible de résoudre l'ID d'univers principal

Pour mettre à jour le lien d'univers

1. Démarrez Universe Designer sur le même ordinateur que celui utilisé pour sauvegarder l'univers personnalisé.
2. Sélectionnez File, Open pour ouvrir votre univers personnalisé.
3. Sélectionnez File, Parameters.

   La boîte de dialogue Universe Parameters s'affiche.
4. Cliquez sur l'onglet Links.
5. Sous la colonne Name, cliquez sur l'univers CA SDM.

   Le bouton Change Source est activé.
6. Cliquez sur le bouton Change Source.

7. Recherchez et sélectionnez l'emplacement du fichier *.unv* de CA SDM.

   Remarque : Le fichier *.unv* est généralement situé dans le dossier CA Universes.

8. Cliquez sur Open, puis sur OK.

   Le lien d'univers est mis à jour.

9. Exportez l'univers personnalisé.

Configuration après la mise à niveau

Vous configurez le produit quand la mise à niveau est terminée. Utilisez l'assistant de configuration pour vérifier vos personnalisations existantes.

Remarque : Si la boîte de dialogue de configuration se ferme sans terminer la configuration post-mise à niveau, exécutez *pdm_configure -s* à partir de la ligne de commande.

Serveurs désactivés autres que les serveurs principaux et secondaires

Après la mise à niveau, tous les serveurs qui n'ont pas été entrés comme serveur principal dans la table usp_servers seront convertis en serveurs secondaires. Avant la mise à niveau, si vous avez ajouté un serveur dans la table usp_servers qui n'est ni serveur principal ni serveur secondaire, désactivez-le après la mise à niveau. Vous pouvez désactiver les serveurs à partir de l'interface utilisateur Web du serveur principal. Pour de plus amples renseignements, consultez l'*Aide en ligne*.

Prise en charge des clients existants à l'aide du serveur EEM 8.4

CA SDM r12.9 utilise le SDK EEM 12.5 est n'est pas compatible avec le serveur EEM 8.4. Pour prendre en charge les clients existants qui utilisent le serveur EEM 8.4, il est nécessaire d'appliquer le correctif du SDK EEM 8.4 sur le serveur CA SDM r12.9. Les détails relatifs à ce correctif sont disponibles auprès du service de soutien de CA.

Mise à niveau de CA Workflow et de CA EEM

Vous installez CA Workflow et CA EEM séparément dans CA SDM r12.9.

Lorsque vous effectuez la migration vers r12.9, effectuez une mise à niveau vers CA EEM r8.4 SP4 et CA Workflow r1.1.132, au minimum.

Remarque : Vous pouvez effectuer une mise à niveau de CA EEM r8.1 directement vers la version r8.4 SP4.

Pour mettre à niveau CA EEM et CA Workflow, exécutez les tâches suivantes :

1. Vérifiez que vous avec effectué la mise à niveau vers CA SDM r12.9.
2. Insérez le support d'installation dans votre lecteur.
3. Installation d'CA EEM
4. Installation de CA Workflow

Après avoir installé CA Workflow et CA EEM, définissez manuellement les options appropriées dans le Gestionnaire d'options. Vérifiez attentivement les options mises à niveau. Le port Tomcat par défaut pour CA Workflow n'est plus le port 8080 et l'URL du gestionnaire de processus par défaut n'est plus pmService.

Remarque : L'option *cawf_pm_url* a été remplacée par la valeur par défaut : *http://<nom_hôte_wf>:<port_tomcat_wf>/pm/service/pmService2*. Vous *devez* donc remplacer manuellement "pmService" par "pmService2" pour que la communication CAWF reste fonctionnelle.

Important : Après la mise à niveau de CA EEM, définissez les options *eiam_hostname*, *use_eiam_artifact* et *use_eiam_authentication* dans Gestionnaire d'options, Sécurité si vous utilisiez auparavant l'authentification utilisateur eIAM CA SDM. Pour en savoir plus sur ces options, consultez l'*Aide en ligne*.

Conservation de la configuration du processus serveur

Dans les précédentes versions de CA SDM, les données relatives à la configuration du processus serveur (créé à l'aide du script pdm_edit.pl) étaient stockées dans le fichier pdm_startup.dat, dans le répertoire $NX_ROOT/samples/pdmconf. Pour conserver cette configuration dans CA SDM r12.9, il est nécessaire de traiter le fichier pdm_startup.dat pour générer cette configuration, qui pourra ensuite être appliquée à l'aide de la commande pdm_configure.

1. Connectez-vous à l'interface utilisateur Web du serveur principal pour y ajouter tous les serveurs secondaires déjà intégrés dans les versions CA SDM antérieures (le cas échéant). Pour de plus amples renseignements, consultez l'*Aide en ligne*.
2. Accédez au répertoire SNX_ROOT/bin et exécutez l'outil de ligne de commande pdm_edit_migration. Cet outil s'applique uniquement à la configuration conventionnelle CA SDM.

   Si l'outil s'exécute correctement, une nouvelle configuration avec état Actif sera créée sinon, une configuration à l'état Inactif sera plutôt créée. Dans l'interface utilisateur Web de CA SDM, vérifiez si la nouvelle configuration est appropriée dans Systèmes, Configuration, onglet Administration. Seules les configurations actives peuvent être appliquées sur un serveur.

   Remarque : Si l'outil ne s'exécute pas correctement, corrigez les entrées posant problème dans le fichier pdm_startup.dat et relancez l'outil.
3. Exécutez le fichier pdm_configure sur le serveur principal pour appliquer cette nouvelle configuration. Pour de plus amples renseignements, reportez-vous à l'*Aide sur la configuration de serveurs*.

Activation de CA SDM et intégration de CA IT PAM

Après la mise à niveau, veillez à intégrer CA SDM dans CA IT PAM 4.0 ou version ultérieure en effectuant les étapes suivantes :

1. Ouvrez CA IT PAM Workflow dans le gestionnaire d'options et modifiez la valeur des options suivantes :
2. Remplacez la valeur de caextwf_processdisplay_url par *http://<wf_hostname>:<wf_tomcat_port>/itpam/Web.jsp?page=runtimeeditor&ROID=*
3. Remplacez également la valeur de caextwf_worklist_url par *http://<wf_hostname>:<wf_tomcat_port>/itpam?page=tasklist*

Important : Lorsque CA SDM est intégré à CA IT PAM qui utilise CA EEM 8.4, vérifiez que vous appliquez le correctif du SDK CA EEM 8.4 sur CA SDM. Les détails relatifs à ce correctif sont disponibles auprès du service de soutien de CA.

Nettoyez le moteur Web et le cache du navigateur

Après avoir effectué la mise à niveau vers CA SDM r12.9, exécutez l'utilitaire pdm_webcache pour nettoyer le cache du moteur Web et du navigateur.

```
pdm_webcache -b -H
```

-b

Avertit l'utilisateur de nettoyer le cache de son navigateur.

-H

Nettoie le cache du moteur Web.

Configuration du directeur Web et des serveurs

À l'issue de la mise à niveau, il est recommandé de configurer les serveurs et le directeur Web.

Pour configurer le directeur Web et les serveurs

Si la version précédente a été configurée pour utiliser des serveurs supplémentaires, ou des directeurs Web, vous pouvez configurer les serveurs et le directeur Web et appliquer la configuration après la mise à niveau.

Pour de plus amples renseignements, reportez-vous au *Manuel d'administration*.

LREL post-migration

Après la migration, procédez aux vérifications suivantes.

1. Interrogez les contenus des nouvelles tables pour vérifier que les tables contiennent les données correctes.
2. Actualisez chaque rapport défini par le site pour vérifier que les données du rapport proviennent des nouvelles tables de LREL.
3. Testez des rapports définis par le site.

Objets et tables désapprouvés

Les objets et les tables suivants sont déconseillés pour cette version de CA SDM. Pendant la migration, le système copie les données dans les tables LREL r12.9. Le système utilise les tables et les objets LREL, mais les anciennes tables conservent, à des fin de référence, les données qui étaient présentes au moment de la mise à niveau.

Remarque : Pour plus d'informations sur les tables LREL, reportez-vous au *Manuel de référence technique*.

Nom du SGBD	Nom de l'objet
Attachment_Lrel	attmnt_lrel
Business_Management_Repository_ Lrel	bmlrel
Chgcat_Group	chgcat_grp
Chgcat_Loc	chgcat_loc
Chgcat_Workshift	chgcat_workshift
Group_Loc	grp_loc
Isscat_Group	isscat_grp
Isscat_Loc	isscat_loc
Isscat_Workshift	isscat _workshift
Knowledge_Lrel_Table	kmlrel
Lrel_Table	lrel1
Pcat_Group	pcat_grp
Pcat_Loc	pcat_loc
Pcat_Workshift	pcat_workshift
Wftpl_Group	wftpl_grp

Tables et objets de LREL

La migration crée automatiquement les tables et objets suivants pour gérer des relations de données plusieurs-à-plusieurs :

Nom du SGBD	Nom de l'objet
usp_lrel_asset_chgnr	lrel_asset_chgnr
usp_lrel_asset_issnr	lrel_asset_issnr
usp_lrel_att_cntlist_macro_ntf	lrel_att_cntlist_macro_ntf
usp_lrel_att_ctplist_macro_ntf	lrel_att_ctplist_macro_ntf
usp_lrel_att_ntflist_macro_ntf	lrel_att_ntflist_macro_ntf
usp_lrel_attachments_changes	lrel_attachments_changes
usp_lrel_attachments_issues	lrel_attachments_issues
usp_lrel_attachments_requests	lrel_attachments_requests
usp_lrel_aty_events	lrel_aty_events

usp_lrel_bm_reps_assets	lrel_bm_reps_assets
usp_lrel_bm_reps_bmhiers	lrel_bm_reps_bmhiers
usp_lrel_cenv_cntref	lrel_cenv_cntref
usp_lrel_dist_cntlist_mgs_ntf	lrel_dist_cntlist_mgs_ntf
usp_lrel_dist_ctplist_mgs_ntf	lrel_dist_ctplist_mgs_ntf
usp_lrel_dist_ntflist_mgs_ntf	lrel_dist_ntflist_mgs_ntf
usp_lrel_false_action_act_f	lrel_false_action_act_f
usp_lrel_false_bhv_false	lrel_false_bhv_false
usp_lrel_kwrds_crsolref	lrel_kwrds_crsolref
usp_lrel_notify_list_cntchgntf	lrel_notify_list_cntchgntf
usp_lrel_notify_list_cntissntf	lrel_notify_list_cntissntf
usp_lrel_notify_list_cntntf	lrel_notify_list_cntntf
usp_lrel_ntfr_cntlist_att_ntfrlist	lrel_ntfr_cntlist_att_ntfrlist
usp_lrel_ntfr_ctplist_att_ntfrlist	lrel_ntfr_ctplist_att_ntfrlist
usp_lrel_ntfr_macrolist_att_ntfrlist	lrel_ntfr_macrolist_att_ntfrlist
usp_lrel_ntfr_ntflist_att_ntfrlist	lrel_ntfr_ntflist_att_ntfrlist
usp_lrel_oenv_orgref	lrel_oenv_orgref
usp_lrel_status_codes_tsktypes	lrel_status_codes_tsktypes
usp_lrel_svc_grps_svc_chgcat	lrel_svc_grps_svc_chgcat
usp_lrel_svc_grps_svc_isscat	lrel_svc_grps_svc_isscat
usp_lrel_svc_grps_svc_pcat	lrel_svc_grps_svc_pcat
usp_lrel_svc_grps_svc_wftpl	lrel_svc_grps_svc_wftpl
usp_lrel_svc_locs_svc_chgcat	lrel_svc_locs_svc_chgcat
usp_lrel_svc_locs_svc_groups	lrel_svc_locs_svc_groups
usp_lrel_svc_locs_svc_isscat	lrel_svc_locs_svc_isscat
usp_lrel_svc_locs_svc_pcat	lrel_svc_locs_svc_pcat
usp_lrel_svc_schedules_chgcat_svc	lrel_svc_schedules_chgcat_svc
usp_lrel_svc_schedules_isscat_svc	lrel_svc_schedules_isscat_svc
usp_lrel_svc_schedules_pcat_svc	lrel_svc_schedules_pcat_svc
usp_lrel_true_action_act_t	lrel_true_action_act_t
usp_lrel_true_bhv_true	lrel_true_bhv_true

Vérifier la conversion de LREL

Pendant la migration des données, le système ajoute des tables LREL pour gérer les relations plusieurs-à-plusieurs. Vous pouvez vérifier le contenu des nouvelles tables et mettre à jour le code et les rapports définis par le site.

Pour vérifier des données dans les tables LREL

1. Interrogez le contenu des tables pour vérifier que celles-ci contiennent les données correctes.
2. Actualisez chaque rapport défini par le site pour vérifier que les données du rapport proviennent des nouvelles tables de LREL.
3. Mettez les requêtes à jour avec les nouvelles références de tables du SGBD.
4. Testez les rapports et le code définis par le site. Mettez votre code à jour pour utiliser les nouvelles tables LREL et une interface prise en charge, par exemple les services Web. Si nécessaire, mettez à jour les noms des tables dans votre code.

Vérification des personnalisations de la base de données

Vous pouvez vérifier que vos personnalisations de base de données ont migré correctement vers la version actuelle du produit.

Pour vérifier les personnalisations de la base de données

1. Examinez chaque table personnalisée à l'aide du produit de gestion de bases de données ou de l'outil de conception Web.
2. Vérifiez que vos fichiers personnalisés figurent dans le répertoire suivant :

   $NX_ROOT/site/mods/

Vérifier les personnalisations des formulaires Web

Vous pouvez vérifier que vos personnalisations de formulaires Web fonctionnent correctement dans la version actuelle du produit.

Pour vérifier les personnalisations des formulaires Web

1. Vérifiez que vos formulaires personnalisés apparaissent dans le répertoire *$NX_ROOT/site/mods/www/htmpl*.
2. Vérifiez que votre formulaire Web s'ouvre correctement dans un navigateur.
3. Vérifiez que le formulaire Web s'ouvre correctement dans l'outil de conception Web.

Modification des types d'accès

Lorsque vous effectuez une mise à niveau à partir de CA SDM r11.2, le processus de mise à niveau crée automatiquement des rôles pour tous les types d'accès et affecte correctement des droits d'accès et des autorisations aux rôles. Si vous souhaitez profiter des nouveaux rôles dans r12.9, vous pouvez créer des rôles pour les types d'accès.

Pour créer des rôles pour des types d'accès

1. Connectez-vous à l'interface Web comme utilisateur avec la possibilité d'accéder à l'onglet Administration.
2. Cliquez sur l'onglet Administration.
3. Dans l'arborescence à gauche, sélectionnez Gestion des rôles et de la sécurité, Types d'accès.

   Tous les types d'accès disponibles s'affichent.
4. Cliquez sur un type d'accès disponible.

   La page des détails du type d'accès s'affiche.
5. Cliquez sur l'onglet Rôles.
6. Sélectionnez un nouveau rôle pour le type d'accès et cliquez sur Mettre à jour les rôles.

   Le nouveau rôle est associé au type d'accès.

   Remarque : Vous pouvez aussi créer un rôle personnalisé et l'affecter au type d'accès. Pour plus d'informations sur la création des rôles, reportez-vous au *Manuel d'administration*.

Activer le calcul de la priorité

Le calcul de la priorité est un ensemble de valeurs qui définit automatiquement les valeurs des options Priorité, Urgence et Impact pour les problèmes et les incidents. Pour les nouvelles installations de CA SDM, le calcul de la priorité par défaut est activé pour les types de tickets de problème et d'incident par défaut. Pourtant, si vous procédez à une mise à niveau depuis une version précédente, le calcul de la priorité par défaut est désactivé.

Si vous créez et activez un calcul de la priorité différent, les valeurs de ticket reflètent les paramètres du calcul de priorité activé qui est associé à un incident ou à un problème. Si aucun calcul de priorité n'est activé, les utilisateurs peuvent définir manuellement la priorité et les autres valeurs des tickets.

Remarque : Les formulaires personnalisés sur les interfaces Employé et Client fonctionnent de la même manière que dans les versions précédentes. Les utilisateurs du libre-service peuvent modifier directement la priorité indépendamment des paramètres du calcul de la priorité.

Pour activer le calcul de la priorité après la migration, procédez de la manière suivante :

1. Sur l'onglet Administration, accédez à Service Desk, Demande/Incidents/Problèmes, Calcul de la priorité.

   La liste des calculs de la priorité s'affiche.

2. Cliquez le calcul de la priorité par défaut ou sur un autre calcul de la priorité et sélectionnez Modifier dans le menu contextuel.

   La page Mettre à jour le calcul de la priorité s'affiche.

3. Définissez l'état sur Activé.

4. Sélectionnez une ou plusieurs des types de tickets suivants :

   Incidents

   Active ce calcul de la priorité pour gérer les tickets d'incidents. Seul un calcul de la priorité activé peut gérer les incidents.

   Problèmes

   Active ce calcul de la priorité pour gérer les tickets de problèmes. Seul un calcul de la priorité activé peut gérer les incidents.

5. Cliquez sur Enregistrer.

   Les valeurs du calcul de la priorité par défaut s'appliquent aux nouveaux tickets sauf si vous avez activé un autre calcul de la priorité. Sur les nouveaux tickets qui utilisent un calcul de la priorité, le champ Priorité est en lecture seule.

Remarque : Pour plus d'informations sur la définition d'un calcul de la priorité pour des clients hébergés et des tickets, reportez-vous au *Manuel d'administration* et à *l'Aide en ligne*.

Ajout du champ Priorité de l'incident aux incidents

La *priorité de l'incident* correspond à la somme des valeurs d'urgence et d'impact. La priorité de l'incident s'applique uniquement au type de ticket Incident. La valeur Priorité de l'incident apparaît sur les incidents une fois que vous avez installé l'option use_incident_priority et que vous l'avez ajoutée au formulaire de la page Détail de l'incident avec l'Outil de conception Web.

Pour ajouter le champ Priorité de l'incident à un incident, procédez comme suit :

1. Installez l'option de use_incident_priority à partir du Gestionnaire d'options, Gestionnaire de demandes.
2. Servez-vous de l'Outil de conception Web pour ajouter le champ Priorité de l'incident aux pages de détails des incidents.

   La valeur Priorité de l'incident apparaît sur la page Détail de l'incident enregistrée lorsque l'option use_incident_priority est installée. Si l'option use_incident_priority n'est pas installée, la valeur de priorité de l'incident est zéro.

Remarque : L'option use_incident_priority gère uniquement la valeur Priorité de l'incident. Cette option n'est pas associée au calcul de la priorité.

Informations complémentaires :

Définition de la plage d'urgence pour les utilisateurs du libre-service (page 68)

Ajout du champ Urgence aux tickets d'employés

Par défaut, le champ Urgence n'apparaît pas sur les incidents ou demandes d'employés. Vous pouvez néanmoins ajouter le champ Urgence à l'aide de l'option urgency_on_employee.

Remarque : Si vous désinstallez l'option urgency_on_employee et désactivez le calcul de la priorité, le champ Priorité apparaît sur les pages Détail de la demande et Détail de l'incident pour les utilisateurs du libre-service.

Pour ajouter le champ Urgence à des tickets d'employés, installez l'option urgency_on_employee à partir du Gestionnaire d'options, Gestionnaire de demandes. Le champ Urgence apparaît sur les incidents ou les demandes d'employés. Les utilisateurs du libre-service peuvent remplacer la valeur sur l'incident.

Définition des valeurs de ticket pour les utilisateurs du libre-service

Vous pouvez contrôler les valeurs d'urgence et de priorité présentées aux utilisateurs du libre-service. Les propriétés que vous définissiez dans le fichier *Internet. cfg* déterminent les choix proposés aux utilisateurs lorsqu'ils créent ou modifient des tickets.

Pour définir des valeurs de ticket pour des utilisateurs du libre-service, tenez compte des points suivants :

1. Pour chaque valeur de remplacement dans le paramètre *web.cfg*, spécifiez une ou plusieurs valeurs.
2. Pour les valeurs d'urgence (page 69), spécifiez un ou plusieurs chiffres de 0 à 4.

3. Pour les valeurs de priorité (page 70), spécifiez un ou plusieurs chiffres de 1 à 5 ou Aucune.
4. Séparez les valeurs par un espace.
5. Spécifiez que la première valeur figurant dans la liste est la valeur par défaut apparaissant sur les tickets. Si nécessaire, vous pouvez répéter la valeur par défaut dans la liste pour améliorer de la lisibilité.

Informations complémentaires :

Définition de la plage d'urgence pour les utilisateurs du libre-service (page 68)
Valeurs des propriétés d'urgence (page 69)
Définition de la plage de priorité pour les utilisateurs du libre-service (page 69)
Valeurs de la propriété de priorité (page 70)

Définition de la plage d'urgence pour les utilisateurs du libre-service

Pour les incidents et demandes du libre-service, vous pouvez configurer les valeurs d'urgence par défaut dans le fichier *web.cfg*. Quand vous définissez une plage de valeur d'urgence, les utilisateurs du libre-service tels que les employés, les employés VIP ou les invités peuvent définir les valeurs d'urgence sur les tickets. Les choix proposés aux utilisateurs du libre-service dépendent de la plage de valeurs que vous avez définie dans le fichier *web.cfg*.

Pour définir la plage d'urgence pour les utilisateurs du libre-service, procédez comme suit :

1. Ouvrez le fichier w*eb.cfg* dans le répertoire approprié :
   - (Windows) %NX_ROOT%\bopcfg\www\
   - (UNIX) $NX_ROOT/bopcfg/www/
2. Pour chaque paramètre, spécifiez une ou plusieurs valeurs de propriété d'urgence (page 69). Séparez les valeurs par un espace.

   ESCEmpUrg

   Spécifie la façon dont les employés VIP peuvent remplacer l'urgence sur les tickets.

   EmpUrg

   Spécifie la façon dont les employés peuvent remplacer l'urgence sur les tickets.

   AnonymousUrg

   Spécifie les priorités valides pour les tickets créés par des utilisateurs invités.

3. Enregistrez le fichier *web.cfg*.

   Sur les nouveaux tickets, les employés, les employés VIP ou les invités peuvent définir des valeurs d'urgence basées sur la plage de valeurs dans le fichier *web.cfg*.

Exemple : Présenter deux valeurs d'urgence seulement aux invités sur une demande

1. Ouvrez le fichier *web.cfg.*
2. Définissez le paramètre *AnonymousUrg* sur 0 4. Par exemple, AnonymousUrg 0 4.
3. Enregistrez le fichier *web.cfg*.

   Les valeurs d'urgence proposées à l'utilisateur du libre-service sont 1-Dès que possible et 5-Immédiatement. La valeur d'urgence par défaut est 1-Dès que possible.

Valeurs des propriétés d'urgence

Le fichier *web.cfg* contient les paramètres contrôlant la façon dont les utilisateurs du libre-service remplacent l'urgence sur les tickets. Les valeurs suivantes de la propriété d'urgence sont disponibles :

- **0** : permet à l'utilisateur de définir l'urgence sur 1-Dès que possible.
- **1** : permet à l'utilisateur de définir l'urgence sur 2-Prochainement.
- **2** : permet à l'utilisateur de définir l'urgence sur 3-Rapidement.
- **3** : permet à l'utilisateur de définir l'urgence sur 4-Très Rapidement.
- **4** : permet à l'utilisateur de définir l'urgence sur 5-Immédiatement.

Définition de la plage de priorité pour les utilisateurs du libre-service

Vous pouvez définir une plage de priorités valides pour permettre aux utilisateurs du libre-service de remplacer des valeurs de priorité sur des tickets. Lorsque vous définissez la plage de priorités, les clients, les employés ou les invités peuvent définir des valeurs de priorité basées sur la plage de valeurs dans le fichier *web.cfg*.

Pour définir la plage de priorités pour les utilisateurs du libre-service, procédez comme suit :

1. Dans le fichier w*eb.cfg* du répertoire approprié :
   - (Windows) %NX_ROOT%\bopcfg\wwww\
   - (UNIX) $NX_ROOT/bopcfg/wwww/
2. Pour chaque paramètre, spécifiez une ou plusieurs valeurs pour la propriété Priorité (page 70).

   CstPrio

   Spécifie la façon dont les clients peuvent remplacer la priorité sur les tickets.

EmpPrio

Spécifie la façon dont les employés peuvent remplacer la priorité sur les tickets.

AnonymousPrio

Spécifie la façon dont les employés peuvent remplacer la priorité sur les tickets.

3. Enregistrez le fichier *web.cfg*.

   Sur les nouveaux tickets, les clients, les employés ou les invités peuvent définir des valeurs de priorité basées sur la plage de valeurs dans le fichier *web.cfg*.

Exemple : Présenter deux valeurs de priorité seulement aux invités

1. Ouvrez le fichier *web.cfg.*
2. Définissez le paramètre *AnonymousPrio* sur Aucune 4. Par exemple : AnonymousPrio Aucune 4.
3. Enregistrez le fichier *web.cfg*.

   Quand un invité travaille avec des tickets, les valeurs d'urgence sont Aucune ou 4. La valeur par défaut est Aucune.

Valeurs de la propriété de priorité

Le fichier *web.cfg* contient les paramètres contrôlant le remplacement de la priorité d'un ticket par les utilisateurs du libre-service. Les valeurs de la propriété de priorité suivantes sont disponibles :

- **Aucune** : permet à l'utilisateur de définir la priorité sur Aucune.
- **1** : permet à l'utilisateur de définir la priorité sur 1 (priorité la plus élevée).
- **2** : permet à l'utilisateur de définir la priorité sur 2.
- **3** : permet à l'utilisateur de définir la priorité sur 3.
- **4** : permet à l'utilisateur de définir la priorité sur 4.
- **5** : permet à l'utilisateur de définir la priorité sur 5 (priorité la plus basse).

Activer des transitions d'état

Après la mise à niveau, toutes les transitions d'état prédéfinies sont inactives, de sorte que les transitions d'état ne s'appliquent pas. Vous pouvez activer et modifier ces transitions d'état en fonction du flux de transitions d'états de tickets que vous voulez.

Remarque: Toutes les descriptions de codes d'état personnalisés qui apparaissent dans des formulaires de ticket sont conservées pendant le processus de mise à niveau.

Pour activer une transition d'état

1. Sur l'onglet Administration, développez le noeud Service Desk et sélectionnez l'un de types de tickets suivants:
   - Demandes de changement
     - Transitions de demande de changement
   - Demandes client
     - Transitions de demande client
   - Demandes/Incidents/Problèmes :
     - Transitions d'incident
     - Transitions de problème
     - Transitions de demande

   La fenêtre Liste des transitions s'affiche.
2. Sélectionnez Afficher le filtre sur la page répertoriant les transitions.

   La partie supérieure de la page affiche des champs de recherche supplémentaires.
3. Sélectionnez Désactivé dans le champ Etat de l'enregistrement et cliquez sur Rechercher.

   La liste de transitions au bas de la page affiche toutes les transitions inactives.
4. Ouvrez la transition à modifier.
5. Sélectionnez Activé dans la liste déroulante Etat de l'enregistrement.
6. Cliquez sur Enregistrer, Fermer la fenêtre.
7. Cliquez sur Rechercher.

   La liste des transitions affiche le type de transition actif.

Remarque : Pour plus d'informations sur les transitions d'état, consultez le *Manuel d'administration* et *l'Aide en ligne*.

Activer des types de transition

Par défaut, tous les types de transitions prédéfinis distribués avec le produit sont désactivés. Par conséquent, les boutons de transition d'état ne sont pas activés. Vous pouvez activer et modifier ces types de transitions pour les adapter au flux de transitions d'état souhaité.

Pour activer un type de transition

1. Sélectionnez Afficher le filtre sur la page Liste des types de transitions.

   La partie supérieure de la page affiche des champs de recherche supplémentaires.

2. Sélectionnez Désactivé dans le champ Etat de l'enregistrement et cliquez sur Rechercher.

   La Liste des types de transitions affiche tous les types de transitions désactivés.

3. Cliquez avec le bouton droit sur le titre du type de transition et sélectionnez Modifier dans le menu.

4. Sélectionnez Activé dans la liste déroulante Etat de l'enregistrement.

5. Cliquez sur Enregistrer, Fermer la fenêtre.

6. Cliquez sur Rechercher.

   La Liste des types de transitions affiche le type de transition activé.

Personnaliser les domaines d'accès fonctionnel

Une *zone d'accès fonctionnel* est un groupe d'objets vous permettant de limiter l'accès utilisateur. Les versions précédentes de CA SDM incluaient huit groupes d'accès fonctionnel fixes pour limiter l'accès aux composants de code.

Pendant la migration, les groupes d'accès fonctionnel migrent vers de nouveaux domaines d'accès fonctionnel pour chaque rôle. La migration gère automatiquement les modifications de Majic, les données de référence par défaut et le mappage des rôles aux nouveaux domaines d'accès fonctionnel.

Après la migration, vous pouvez procéder de la façon suivante :

- Examinez la façon dont les objets sont mappés aux domaines d'accès fonctionnel nouveaux et existants et aux autorisations par rôle. Utilisez l'Outil de conception Web pour vérifier les domaines d'accès fonctionnel.
- Utilisez CA SDM pour remapper ou modifier des autorisations. Assurez-vous que les utilisateurs disposent d'un accès adéquat aux fonctionnalités et aux objets.

Remarque : Pour plus d'informations sur les autorisations par défaut et sur la façon dont les objets sont mappés vers les nouveaux domaines d'accès fonctionnel, consultez le site Web de soutien du produit. Pour en savoir plus sur la modification ou l'ajout de domaines d'accès fonctionnel, consultez *l'Aide en ligne*.

La table suivante mappe les domaines d'accès fonctionnels aux composants de code.

Domaine d'accès fonctionnel	Composant de code	nouveau
Administration	admin	Non
Incident/Problème/Demande	call_mgr	Non
Demande de changement	change_mgr	Non
Inventaire	inventory	Non

Demande client	issue_mgr	Non
Document de connaissances	kd	Non
Notification	notify	Non
Référence	référence	Non
Sécurité	sécurité	Non
Annonce	annonce	Oui
Références Incident/Problème/Demande	call_mgr_reference	Oui
Modèle Incident/Problème/Demande	call_mgr_template	Oui
Modèle de demande de changement	change_mgr_template	Oui
Référence de la demande de changement	change_reference	Oui
Elément de configuration	ci	Oui
Elément de configuration commun	ci_common_ro	Oui
Référence de l'élément de configuration	ci_reference	Oui
Contact	contact	Oui
Groupe	groupe	Oui
Modèle de demande client	issue_mgr_template	Oui
Référence de la demande client	issue_reference	Oui
Emplacement :	emplacement	Oui
Référence de la notification	notification_reference	Oui
Organisation	Organisation	Oui
Définition de priorités	définition de priorités	Oui
Niveau de service	service_level	Oui
Table Site	site	Oui
Requête stockée	stored_queries	Oui
Enquête	enquête	Oui
Administrateur de clients hébergés	tenant_admin	Oui
Timezone	timezone	Oui
Référence du flux de travaux	workflow_reference	Oui
Horaire	horaires	Oui

Modificiations du niveau d'accès post-migration

Après la migration, vous pouvez vérifier des niveaux d'accès fonctionnel de chaque rôle. Etant donné que les objets ont été déplacés vers d'autres domaines d'accès fonctionnel, l'utilisateur peut avoir accès à certains écrans dans des situations qui, précédemment, le leur interdisaient. Il se peut également qu'ils n'aient plus accès à des formulaires auxquels il avaient précédemment accès. Ces deux situations peuvent se produire quand un nouveau domaine d'accès fonctionnel gère des autorisations pour deux des domaines d'accès fonctionnel d'origine.

Remarque : Pour plus d'informations sur les autorisations par défaut et sur la façon dont les objets sont mappés aux nouveaux domaines d'accès fonctionnel, consultez le site Web de soutien du produit. Pour plus d'informations sur la façon de modifier ou d'ajouter des niveaux d'accès, consultez *l'Aide en ligne*.

Fichier SITEMODS.JS

Les lignes de code ajoutées au fichier sitemods.js de la version antérieure, appelées à partir d'une page HTMPL, doivent être fusionnées dans le fichier sitemods.js actuel pour que le code fonctionne.

Ajustez les types d'accès

Si vous utilisiez des types d'accès et des partitions de données personnalisés dans la version précédente de CA SDM, vous risquez de rencontrer des difficultés avec les paramètres de partition de données Gestion des connaissances après la migration. Cela peut donner lieu à des problèmes liés aux paramètres des groupes d'autorisation d'accès aux catégories et documents. Par exemple, un utilisateur a accès des informations restreintes.

Remarque : Même si vous avez recréé une partition de données ou un type d'accès après l'avoir supprimé, vérifiez vos paramètres de type d'accès et de partition de données après la mise à niveau.

Pour ajuster les types d'accès

1. Cliquez sur l'onglet Administration.

   La page Administration s'affiche.

2. Accédez à Gestion des rôles et de la sécurité, Gestion des rôles, Liste des rôles.

   La liste des rôles s'affiche.

3. Effectuez les opérations suivantes pour chaque rôle :
   a. Cliquez avec le bouton droit sur le dossier, puis sélectionnez Modifier.
   b. Vérifiez le champ Nom de la partition de données sous l'onglet Autorisation.

      Si ce champ est vide, aucune partition de données n'est associée au type d'accès sélectionné, l'utilisateur n'a donc aucune restriction et peut accéder à tous les documents ou à toutes les catégories du produit, même si vous configurez des groupes d'autorisations.

      Cette action peut être appropriée pour les administrateurs, mais pas pour tous les rôles. Si aucune partition de données n'est associée au rôle, vous pouvez en créer ou en modifier une.

Ajuster les paramètres de partition de données

Vous pouvez ajuster les contraintes de partition après avoir configuré les rôles dans votre système. Ajustez les contraintes de partition pour vérifier que les autorisations appropriées fonctionnent correctement après une mise à niveau vers la version actuelle du produit.

Pour ajuster des contraintes de partition de données

1. Sous l'onglet Administration, accédez à Gestion des rôles et de la sécurité, Partitions de données, Contraintes de partition de données.

   La page Liste des contraintes de partition de données s'affiche.

2. Vérifiez les paramètres de contrainte de code Majic pour des tables suivantes :

   SKELETONS

   Spécifie la table utilisé pour les documents de connaissances.

   O_INDEXES

   Spécifie la table utilisait pour les catégories de connaissances.

   Les paramètres de contrainte de table sont vérifiés.

3. Cliquez sur Afficher le filtre et entrez les partitions de données précédemment utilisées.

Remarque : Vous pouvez également utiliser le champ Nom de la table dans la zone de recherche pour limiter votre liste. Par exemple, entrez *SKELETONS* ou *O_INDEXES* dans le champ Nom de la table, puis cliquez sur Rechercher.

Modifiez les systèmes d'aide après la migration des rôles

Après la mise à niveau, CA SDM fournit l'ensemble de l'*Aide en ligne* pour tous les rôles migrés. Vous pouvez modifier les systèmes d'aide d'un rôle, en fonction des besoins de votre système d'aide en ligne.

Pour modifier les systèmes d'aide d'un rôle

1. Sous l'onglet Administration, accédez Gestion des rôles et de la sécurité, Liste des rôles.

   La page Liste des rôles s'affiche.

2. Ouvrez le rôle à modifier (*client*, par exemple).

   La page Détail du rôle s'affiche.

3. Cliquez sur Modifier.

4. Sélectionnez l'onglet Interface Web.

   Cliquez sur Affichage de l'aide.

   La liste des systèmes d'aide disponibles apparaît pour le rôle sélectionné.

5. Sélectionnez un système d'aide, client, par exemple.

6. Enregistrez le rôle.

   Le système d'aide en ligne sélectionné s'affiche désormais pour ce rôle.

Vous pouvez aussi afficher les rubriques disponibles dans un système d'aide en ligne en sélectionnant le détail du système d'aide et en cliquant sur le bouton Affichage de l'aide.

Paramètres par défaut des contraintes

Les paramètres par défaut standard des contraintes sont répertoriés comme suit :

Les paramètres de contrainte pour les partitions de données Client (associé) et Employé (associé)

Les paramètres de contrainte pour les partitions de données Client (associé) et Employé (associé) doivent être définis comme suit :

Table SKELETONS

Contrainte Afficher :

'SKELETONS READ_PGROUP dans @root.pgroups ou READ_PGROUP.[pgroup] contained_roles.role dans @root.id) et ACTIVE_STATE = 0'
Contraintes Pré-mi. à jr. et Supprimer :

'id = 0' (id=0 indique aucun accès)

Table O_INDEXES

Contrainte Afficher :

READ_PGROUP dans @root.pgroups ou READ_PGROUP.[pgroup] contained_roles.role dans @root.id
Contraintes Mise à jour préalable et Supprimer :
WRITE_PGROUP dans @root.pgroups OU WRITE_PGROUP.[pgroup] contained_roles.role DANS @root.role

Les paramètres de contrainte pour l'analyste CA SDM (ou associé), les gestionnaires de connaissances (ou associés) et les ingénieurs Bases de connaissances (ou associés)

Les paramètres de contrainte pour l'analyste CA SDM (ou associé), les gestionnaires de connaissances (ou associés) et les ingénieurs Bases de connaissances (ou associés) doivent être définis comme suit :

Table SKELETONS

Contrainte Afficher :
(ACTIVE_STATE >=0) et (READ_PGROUP dans @root.pgroups OU (ACTIVE_STATE > 0 ET ASSIGNEE_ID = @root.id) OU (ACTIVE_STATE = 0 ET OWNER_ID = @root.id)) Activé

Contraintes Mise à jour préalable et Supprimer :
(ACTIVE_STATE >= 0) ET (WRITE_PGROUP dans @root.pgroups OU (ACTIVE_STATE > 0 ET ASSIGNEE_ID = @root.id) OU (ACTIVE_STATE = 0 ET OWNER_ID= @root.id)) Activé

Table O_INDEXES

Contrainte Afficher :
READ_PGROUP dans @root.pgroups READ PGROUP_PGROUP.[pgroup] contained_roles.role dans @root.role

Contraintes Mise à jour préalable et Supprimer :
WRITE_PGROUP dans @root.pgroups OU WRITE_PGROUP.[pgroup] contained_roles.role DANS @root.role

Démarrez l'interface Web IIS (CAisd)

Après avoir mis à niveau une installation de r11.2 sous Windows avec intégration IIS, l'interface Web IIS de CA SDM (CAisd) sera arrêtée. Si vous voulez continuer à utiliser l'intégration IIS, démarrez manuellement CAisd après la mise à niveau.

Important : Si vous voulez utiliser IIS 7.0, vous *devez* installer les composants CGI et Metabase Compatability.

Modification des formulaires HTMPL personnalisés

Après la mise à niveau de CA SDM, modifiez tous les formulaires HTMPL personnalisés qui contenaient des contrôles de carnet pour inclure les macros Web et spécifier les noms de groupe d'onglets appropriés.

Pour chaque formulaire personnalisé, utilisez l'outil de conception Web pour modifier les instructions de <PDM_NOTEBOOK> en <PDM_MACRO name=startNotebook> et les instructions de <PDM_TAB> en <PDM_MACRO name=TAB>.

Remarque : Pour plus d'informations sur l'utilisation de l'outil de conception Web, reportez-vous à l'*Aide en ligne de l'outil de conception Web*.

Mise à niveau de Gestion des connaissances à partir de r11.2

La mise à niveau de CA SDM r12.9 vers r11.2 met automatiquement à niveau votre environnement Gestion des connaissances. À la fin de la mise à niveau, effectuez les opérations suivantes :

1. Mappez les liens créés dans une résolution d'un document vers la base de données pour localiser les liens rompus.

   Remarque : Utilisez la politique *Indiquer les liens rompus* par défaut pour localiser les liens rompus.

2. Dans l'onglet Administration, sélectionnez Connaissances, Politiques d'automatisation et Planification.

   La page Politiques d'automatisation s'ouvre.

3. Cochez la case Run the Automated Policies calculation.
4. Sélectionnez l'intervalle pour effectuer le calcul et cliquez sur Enregistrer.

   Les politiques seront traitées à la date et à l'heure indiquées.

5. Dans l'onglet Administration, sélectionnez Connaissances, Système et Paramètres généraux.

   La page Système s'ouvre.

6. Spécifiez les renseignements suivants :

   Chemin d'accès aux fichiers d'index EBR

   Définit l'emplacement de stockage des fichiers d'index EBR. CA SDM crée des fichiers d'index EBR lorsque vous enregistrez et publiez un document de connaissances. Selon votre type de configuration, considérez les points suivants lors de la définition du chemin d'accès aux fichiers d'index EBR :

   - Conventionnelle : si vous procédez à la mise à niveau vers CA SDM r12.9 à partir de la version r11.2 ou r12.X, vous pouvez ne pas utiliser un chemin d'accès partagé UNC. Si vous n'avez pas créé de chemin d'accès UNC, CA SDM utilise le chemin d'accès par défaut pour stocker les fichiers d'index EBR. Si vous utilisez un lecteur partagé UNC, copiez manuellement les dossiers ebr/ebr_ADM de l'emplacement par défaut ($NX_ROOT/site/) vers le chemin d'accès partagé UNC.
   - Disponibilité avancée : si vous procédez à la mise à niveau vers la configuration de disponibilité avancée à partir de la version r11.2 ou r12.X de CA SDM, vous devez créer des chemins d'accès partagés UNC et les utiliser pour stocker les fichiers d'index EBR. L'information d'authentification UNC n'est pas requise pour le chemin d'accès par défaut. Si vous utilisez un chemin d'accès UNC, copiez manuellement les dossiers ebr/ebr_ADM de l'emplacement par défaut ($NX_ROOT/site/) vers le chemin d'accès partagé UNC.

   Important : Le chemin d'accès aux fichiers d'index EBR et le chemin d'accès aux fichiers KEIT doivent faire référence aux mêmes informations d'authentification UNC et le chemin d'accès doit résider sur le même serveur pour permettre leur prise en charge.

   Valeur par défaut : $NX_ROOT/site/ebr

   Chemin d'accès aux fichiers d'importation/exportation de connaissances

   Définit l'emplacement de stockage des trousses d'importation/exportation KEIT pendant une opération d'importation/exportation. Selon votre type de configuration, considérez les points suivants lors de la définition du chemin d'accès aux fichiers KEIT :

   - Conventionnelle : si vous procédez à la mise à niveau vers CA SDM r12.9 à partir de la version r11.2 ou r12.X, vous pouvez ne pas utiliser un chemin d'accès partagé UNC. Si vous n'avez pas créé de chemin d'accès UNC, CA SDM utilise le chemin d'accès par défaut pour stocker les fichiers KEIT. Si vous utilisez un lecteur partagé UNC, copiez manuellement les dossiers de trousses d'importation/exportation de l'emplacement par défaut ($NX_ROOT/site/keit) vers le chemin d'accès partagé UNC.

- Disponibilité avancée : si vous procédez à la mise à niveau vers la configuration de disponibilité avancée à partir de la version r11.2 ou r12.X de CA SDM, vous devez créer des chemins d'accès partagés UNC et les utiliser pour stocker les fichiers KEIT. L'information d'authentification UNC n'est pas requise pour le chemin d'accès par défaut. Si vous utilisez un chemin d'accès UNC, copiez manuellement les dossiers de trousses d'importation/exportation de l'emplacement par défaut ($NX_ROOT/site/keit) vers le chemin d'accès partagé UNC.

Important : Le chemin d'accès aux fichiers d'index EBR et le chemin d'accès aux fichiers KEIT doivent faire référence aux mêmes informations d'authentification UNC et le chemin d'accès doit résider sur le même serveur pour permettre leur prise en charge.

Valeur par défaut : $NX_ROOT/site/keit

Information d'authentification UNC

Vous pouvez utiliser cette option pour créer l'information d'authentification UNC afin d'accéder au lecteur réseau partagé pour accéder aux fichiers d'indexation EBR et aux trousses d'importation/exportation. Utilisez le lien Informations d'authentification UNC pour créer cette information.

Remarque : Les chemins d'accès UNC et l'information d'authentification UNC sont requis dans le cadre de la configuration de disponibilité avancée. Redémarrez le service CA SDM lorsque vous modifiez l'un des détails UNC (chemins d'accès UNC ou information d'authentification UNC). Pour de plus amples renseignements sur la création de l'information d'authentification UNC, reportez-vous à l'*Aide en ligne*.

7. Exécutez pdm_k_reindex comme suit :

pdm_k_reindex -pm

Corrige les liens de documents et les images incorporées dans le champ de résolution.

Important : Après la mise à niveau, une erreur critique peut survenir lors de l'exécution de *pdm_k_reindex -pm*. Le cas échéant, parcourez les répertoires Connaissances, Gestionnaire de processus d'approbation, Paramètres du processus d'approbation et modifiez la valeur l'option *Autorisations de modification d'un document après sa publication* en choisissant *Les utilisateurs disposant de droits d'accès complets peuvent modifier des documents*, puis exécutez pdm_k_reindex -pm.

pdm_k_reindex -ml

Corrige les liens de documents à l'intérieur du champ de résolution et les mappe à la base de données.

pdm_k_reindex

Indexe les documents pour qu'ils puissent faire l'objet d'une recherche dans votre environnement de connaissances.

L'environnement de Gestion des connaissances est mis à niveau vers r12.9.

Remarque : Après la mise à niveau, l'impression de documents de connaissances peut entraîner l'insertion d'un grand espace après la section Résolution du document. Cet espace est inséré en raison d'un problème avec la mise à niveau de modèles de document à partir d'une version antérieure. Pour de plus amples renseignements sur la résolution de ce problème d'impression, consultez les *Notes de parution*.

Important : Après la mise à niveau, les données de notification de Gestion des connaissances des versions précédentes de CA SDM utilisent le moteur de notification de r12.9. Ainsi, il y a par exemple des notifications d'activité par défaut et des règles de notification pour des types d'objets, comme la Fiche de rapport des connaissances.

Mise à niveau de Gestion des connaissances à partir de CA SDM r12.x

Une mise à niveau vers CA SDM r12.9 depuis la version r12 ou r12.1 met automatiquement à niveau votre environnement Gestion des connaissances. À la fin de la mise à niveau, effectuez les opérations suivantes :

1. Mappez les liens créés dans une résolution d'un document vers la base de données pour localiser les liens rompus.

   Remarque : Utilisez la politique *Indiquer les liens rompus* par défaut pour localiser les liens rompus.

2. Sous l'onglet Administration, accédez à Connaissances, Politiques d'automatisation, Politiques, Planification.

   La page Planification apparaît.

3. Sélectionnez la case à cocher Exécuter le calcul des politiques d'automatisation dans le champ Dernière mise à jour.

4. Entrez une date dans la zone de texte Planification ou cliquez sur l'icône Calendrier pour sélectionner une date.

5. Sélectionnez l'intervalle pour effectuer le calcul et exécuter les politiques.

6. Cliquez sur Enregistrer.

   Les politiques sont traitées à la date et à l'heure spécifiées.

7. Sous l'onglet Administration, accédez à Connaissances, Systèmes, Paramètres généraux.

   La page Paramètres généraux s'ouvre.

8. Spécifiez les renseignements suivants :

   Chemin d'accès aux fichiers d'index EBR

   Définit l'emplacement de stockage des fichiers d'index EBR. CA SDM crée des fichiers d'index EBR lorsque vous enregistrez et publiez un document de connaissances. Selon votre type de configuration, considérez les points suivants lors de la définition du chemin d'accès aux fichiers d'index EBR :

   - Conventionnelle : si vous procédez à la mise à niveau vers CA SDM r12.9 à partir de la version r11.2 ou r12.X, vous pouvez ne pas utiliser un chemin d'accès partagé UNC. Si vous n'avez pas créé de chemin d'accès UNC, CA SDM utilise le chemin d'accès par défaut pour stocker les fichiers d'index EBR. Si vous utilisez un lecteur partagé UNC, copiez manuellement les dossiers ebr/ebr_ADM de l'emplacement par défaut ($NX_ROOT/site/) vers le chemin d'accès partagé UNC.
   - Disponibilité avancée : si vous procédez à la mise à niveau vers la configuration de disponibilité avancée à partir de la version r11.2 ou r12.X de CA SDM, vous devez créer des chemins d'accès partagés UNC et les utiliser pour stocker les fichiers d'index EBR. L'information d'authentification UNC n'est pas requise pour le chemin d'accès par défaut. Si vous utilisez un chemin d'accès UNC, copiez manuellement les dossiers ebr/ebr_ADM de l'emplacement par défaut ($NX_ROOT/site/) vers le chemin d'accès partagé UNC.

   Important : Le chemin d'accès aux fichiers d'index EBR et le chemin d'accès aux fichiers KEIT doivent faire référence aux mêmes informations d'authentification UNC et le chemin d'accès doit résider sur le même serveur pour permettre leur prise en charge.

   Valeur par défaut : $NX_ROOT/site/ebr

   Chemin d'accès aux fichiers d'importation/exportation de connaissances

   Définit l'emplacement de stockage des trousses d'importation/exportation KEIT pendant une opération d'importation/exportation. Selon votre type de configuration, considérez les points suivants lors de la définition du chemin d'accès aux fichiers KEIT :

   - Conventionnelle : si vous procédez à la mise à niveau vers CA SDM r12.9 à partir de la version r11.2 ou r12.X, vous pouvez ne pas utiliser un chemin d'accès partagé UNC. Si vous n'avez pas créé de chemin d'accès UNC, CA SDM utilise le chemin d'accès par défaut pour stocker les fichiers KEIT. Si vous utilisez un lecteur partagé UNC, copiez manuellement les dossiers de trousses d'importation/exportation de l'emplacement par défaut ($NX_ROOT/site/keit) vers le chemin d'accès partagé UNC.

- Disponibilité avancée : si vous procédez à la mise à niveau vers la configuration de disponibilité avancée à partir de la version r11.2 ou r12.X de CA SDM, vous devez créer des chemins d'accès partagés UNC et les utiliser pour stocker les fichiers KEIT. L'information d'authentification UNC n'est pas requise pour le chemin d'accès par défaut. Si vous utilisez un chemin d'accès UNC, copiez manuellement les dossiers de trousses d'importation/exportation de l'emplacement par défaut ($NX_ROOT/site/keit) vers le chemin d'accès partagé UNC.

  Important : Le chemin d'accès aux fichiers d'index EBR et le chemin d'accès aux fichiers KEIT doivent faire référence aux mêmes informations d'authentification UNC et le chemin d'accès doit résider sur le même serveur pour permettre leur prise en charge.

  Valeur par défaut : $NX_ROOT/site/keit

  Information d'authentification UNC

  Vous pouvez utiliser cette option pour créer l'information d'authentification UNC afin d'accéder au lecteur réseau partagé pour accéder aux fichiers d'indexation EBR et aux trousses d'importation/exportation. Utilisez le lien Informations d'authentification UNC pour créer cette information.

  Remarque : Les chemins d'accès UNC et l'information d'authentification UNC sont requis dans le cadre de la configuration de disponibilité avancée. Redémarrez le service CA SDM lorsque vous modifiez l'un des détails UNC (chemins d'accès UNC ou information d'authentification UNC). Pour de plus amples renseignements sur la création de l'information d'authentification UNC, reportez-vous à l'*Aide en ligne*.

9. (Pour les mises en oeuvre de la recherche par mot clé) Lorsque vous y êtes invité, entrez la commande suivante :

   ```
   pdm_k_reindex factory:all
   ```

   Important : La variable *all* est sensible à la casse. Si vous utilisez factory:ALL, les erreurs s'afficheront dans les fichiers journaux.

   L'environnement de Gestion des connaissances est mis à niveau vers r12.9.

Remarque : Après la mise à niveau, l'impression de documents de connaissances peut entraîner l'insertion d'un grand espace après la section Résolution du document. Cet espace est inséré en raison d'un problème avec la mise à niveau de modèles de document à partir d'une version antérieure. Pour de plus amples renseignements sur la résolution de ce problème d'impression, consultez les *Notes de parution*.

Important : Après la mise à niveau, les données de notification de Gestion des connaissances des versions précédentes de CA SDM utilisent le moteur de notification de r12.9. Ainsi, il y a par exemple des notifications d'activité par défaut et des règles de notification pour des types d'objets, comme la Fiche de rapport des connaissances.

Chapitre 3: Planification

Ce chapitre traite des sujets suivants :

Liste des ports par défaut et des ports recommandés CA SDM (page 85)
Procédure de planification de la disponibilité avancée (page 88)
Planification de l'installation de CA MDB (page 99)
Planification de l'installation de CA SDM (page 102)
Planification de l'installation de CA NSM (page 116)
Planification de l'installation de CA EEM et CA Workflow (page 116)
Planification d'intégration de CA Process Automation (page 123)
Planification de l'installation de CA Business Intelligence (page 127)
Stratégies de mise en oeuvre (page 133)
Activer l'authentification Windows dans Firefox (page 134)

Liste des ports par défaut et des ports recommandés CA SDM

L'installation de CA SDM requiert l'ouverture de divers ports et plages de ports sur votre pare-feu. Les informations sur ces ports aident les administrateurs du site et de la sécurité à installer et à configurer CA SDM, tout en facilitant les intégrations avec d'autres solutions CA Technologies et les produits tiers.

Les ports à ouvrir sur votre pare-feu dépendent des paramètres du fichier *NX.env*. Par défaut, CA SDM choisit le port approprié en fonction de la disponibilité. Le système réserve les ports inférieurs à 1024, mais peut demander un numéro de port aussi élevé que 65335.

Les variables *NX.env* suivantes définissent le port de départ (2100) et la valeur d'augmentation (plus 1) que le système utilise pour rechercher un port ouvert pour le démarrage du processus :

- NX_SLUMP_FIXED_SOCKETS=1
- NX_SLUMP_SECONDARY_SOCKET=2100

La liste suivante affiche les ports par défaut et recommandés (ainsi que les plages de ports) pour une installation standard de CA SDM :

Base de données

- Oracle : 1521
- SQL Server : 1433

CA SDM

- FTP : 21
- SMTP : 25

- HTTP : 80
- HTTPS : 8080
- HTTPS (secondaire) : 8081
- POP3 : 110
- IMAP : 143
- LDAP : 389
- WebEx : 1270
- mstsc : 1389
- oaserver : 1706
- Connecteur logiciel slump : 2100
- qserver : 2234
- Connecteur logiciel de l'utilitaire de surveillance : 2300
- Communications : 2365
- Apache Tomcat : 8080
- Arrêt Apache Tomcat :
- SSL sur Apache Tomcat : 8443

CA CMDB

- Visualiseur : 9080
- Arrêt Visualiseur Apache Tomcat : 9085
- CA Cohesion ACM : 9000
- Arrêt CA Cohesion ACM Tomcat : 9005

CA EEM

Port d'administration : 5250

CA Workflow

- Apache Tomcat : 8090
- Arrêt Apache Tomcat : 8095

REST

- Apache Tomcat : 8050
- Arrêt Apache Tomcat : 8055

CA Business Intelligence

Remarque : Pour plus d'informations sur le traitement des ports du pare-feu pour BusinessObjects, reportez-vous au manuel BusinessObjects Enterprise XI r2 Deployment and Configuration Guide.

- Apache Tomcat : 8080

  Recommandé : 8070
- Redirection Apache Tomcat : 8443
- Arrêt Apache Tomcat : 8075
- Arrêt Apache Tomcat secondaire : 8005
- Pilote ODBC : 1706
- BusinessObjects Central Management Server (CMS) : 8080
- Serveur d'applications BusinessObjects : 6400
- ODBC DSN (base de données OpenAcess) : 1706
- BEA WebLogic : 7001

Moteur de recherche EBR

- Port de base : 13000

Serveur de portail

- Apache Tomcat : 8080
- Arrêt Apache Tomcat : 8085
- Fonctionnalité SSL : 8443
- Portal_Safe_List : 8444

Automatisation du soutien

- Serveur principal (serveur de connecteur logiciel) interne : 7005
- Serveur principal (serveur de connecteur logiciel) externe : 10443
- Serveur mandataire de connecteur logiciel (serveur principal de configuration de connecteur logiciel) interne : 7005
- Serveur mandataire de connecteur logiciel (serveur principal de configuration de connecteur logiciel) externe : 10444
- Serveur de routage de message (configuration de connecteur logiciel) externe : 10444
- Apache Tomcat : 8070
- Arrêt Apache Tomcat : 8075

Visualiseur

- Apache Tomcat : 9080
- Arrêt Apache Tomcat : 9085

Procédure de planification de la disponibilité avancée

La configuration de la disponibilité avancée offre une meilleure résistance aux interruptions de serveur, une meilleure disponibilité des applications et qui prend en charge la maintenance progressive avec une interruption minimale pour les utilisateurs finals. Cette configuration nécessite un serveur d'arrière-plan, un ou plusieurs serveurs de secours et un ou plusieurs serveurs d'applications. La configuration précédente incluant un serveur principal et un serveur secondaire est désormais appelée configuration conventionnelle.

Vous pouvez configurer CA SDM pour utiliser la configuration conventionnelle ou la configuration de disponibilité avancée. Vous pouvez également passer d'une configuration à l'autre.

La configuration de disponibilité avancée améliore la disponibilité globale de CA SDM comme suit :

- Elle réduit le temps d'indisponibilité des applications CA SDM causé par une défaillance d'application, une défaillance matérielle, ou la maintenance, en réduisant le point unique de défaillance.
- Elle réduit le temps d'indisponibilité de CA SDM en prenant en charge la maintenance progressive des serveurs. Ainsi, les utilisateurs peuvent continuer à travailler sur l'application pendant que l'un des serveurs se trouve en maintenance.

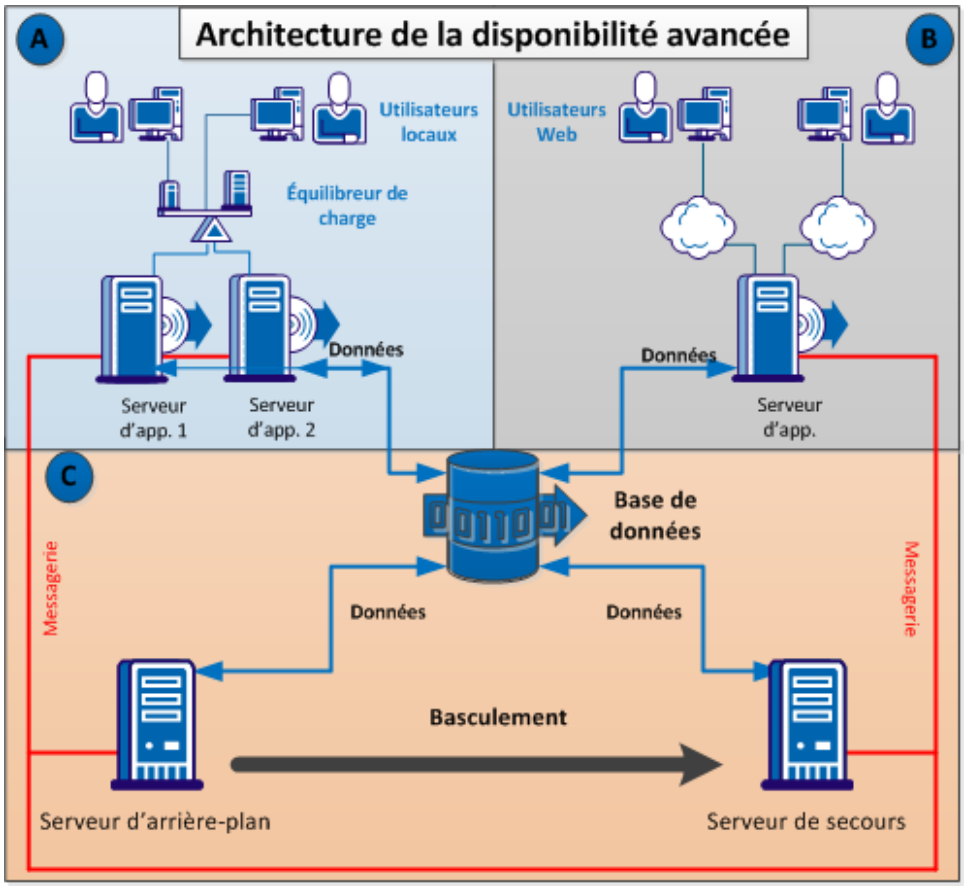
Pour de plus amples renseignements sur la planification et la configuration de la disponibilité avancée, reportez-vous au *Manuel de mise en oeuvre* ou consultez les scénarios s'y rapportant dans la bibliothèque.

Avant de configurer la disponibilité avancée, vérifiez les remarques sur la planification suivantes :

- Architecture CA SDM pour la disponibilité avancée (page 89)
- Choix de la configuration de disponibilité avancée (page 91)
- Remarques sur la configuration de disponibilité avancée (page 91)

Architecture CA SDM pour la disponibilité avancée

La configuration de disponibilité avancée inclut un serveur d'arrière-plan, un ou plusieurs serveurs de secours et un ou plusieurs serveurs d'applications. Pour réduire le point de défaillance unique, chaque serveur dispose d'une connexion directe avec la base de données. Tous les composants de l'architecture communiquent à l'aide d'un protocole CA interne. Le schéma suivant illustre un exemple de mise en oeuvre de CA SDM :



L'architecture est développée sur trois emplacements différents : A, B et C. L'emplacement A dispose de deux serveurs d'applications, servant les utilisateurs à travers un équilibreur de charge. L'emplacement B dispose d'un serveur d'applications servant directement les utilisateurs, et l'emplacement C dispose du serveur d'arrière-plan, du serveur de secours et de la base de données. Chaque serveur dispose d'une connexion directe à la base de données. Les lignes bleues indiquent le flux vers et à partir de la base de données. Les lignes rouges identifient la communication interne entre les composants.

Serveur d'arrière-plan

Le serveur d'arrière-plan est le noyau de l'architecture de disponibilité avancée. Ce serveur fournit des services auxiliaires à d'autres serveurs et exécute tous les processus singleton de CA SDM. Un processus peut être désigné comme singleton lorsqu'un seul exemplaire de ce processus peut être actif dans une installation SDM. Seuls les utilisateurs disposant du type d'accès administrateur peuvent accéder au serveur d'arrière-plan. Pour améliorer la disponibilité, le serveur de secours effectue une copie shadow du serveur d'arrière-plan. Vous pouvez définir le serveur de secours comme serveur d'arrière-plan en cas de panne ou lors d'une maintenance progressive.

Serveur de secours

La fonction principale du serveur de secours est d'agir en tant que serveur de secours actif pour le serveur d'arrière-plan. Le serveur de secours dispose du même matériel et de la même plate-forme de système d'exploitation que le serveur d'arrière-plan. Le serveur de secours peut exécuter tous les processus exécutés sur le serveur d'arrière-plan. Le serveur de secours reste inactif lors du fonctionnement normal du système, mais il continue de mettre à jour les caches critiques en écoutant les messages internes du système de CA SDM pour détecter les changements de base de données. Si le serveur d'arrière-plan échoue ou requiert une maintenance progressive, vous pouvez le remplacer par le serveur de secours avec une interruption minimale des serveurs d'applications ainsi que des utilisateurs finals. Vous pouvez appeler un utilitaire pour effectuer cette permutation.

Le serveur de secours exécute uniquement un sous-ensemble limité des processus normalement exécutés sur le serveur d'arrière-plan. Vous ne pouvez pas vous connecter à l'interface Web sur le serveur de secours.

Serveur d'applications

Le serveur d'applications dispose de tous les composants CA SDM nécessaires aux utilisateurs finals à travers diverses interfaces telles que des services Web, SOAP et RESTful. Les serveurs d'applications sont indépendants les uns des autres et résistants aux interruptions de serveur d'arrière-plan pendant de courtes périodes. Les utilisateurs ont accès aux serveurs d'applications. Vous pouvez supprimer les serveurs d'applications séparément et revenir au service à l'aide de la nouvelle fonctionnalité de mise au repos. Cette fonctionnalité de mise au repos permet aux utilisateurs de terminer leur travail, puis de se connecter à un autre serveur d'applications.

Choix de la configuration de disponibilité avancée

La configuration de disponibilité avancée fournit une disponibilité supérieure, réduit les durées et prend en charge la maintenance progressive. Prévoyez la configuration de disponibilité avancée lorsque l'une des conditions suivantes est vérifiée :

- Vous avez besoin d'un degré élevé de disponibilité de CA SDM.
- Les serveurs CA SDM doivent être plus indépendants et résistants aux défaillances.
- Vous devez pouvoir supprimer et renvoyer les serveurs de CA SDM au service, sans arrêter l'intégralité de l'installation de CA SDM.
- Vous exigez un temps d'indisponibilité quasi nul pendant la maintenance progressive.

Remarques sur la configuration de disponibilité avancée

Avant de décider d'implémenter la configuration de disponibilité avancée, il est recommandé de prendre en compte les points suivants :

Remarques générales

Toutes les remarques sur la planification de la configuration conventionnelle sont valables pour la configuration de disponibilité avancée. Pour de plus amples renseignements sur la planification de la configuration conventionnelle, reportez-vous au *Manuel de mise en oeuvre*.

- Des coûts de matériel supplémentaires sont à prévoir, car un serveur d'arrière-plan, au moins un serveur de secours et un ou plusieurs serveurs d'applications sont nécessaires. La configuration des serveurs de secours et d'arrière-plan doit être identique.
- Un serveur de base de données distant et un serveur pour le partage de fichiers d'index d'outils de connaissances, de fichiers d'importation/exportation d'outils de connaissances, de fichiers de sortie de purge et d'archivage et de référentiels de pièces jointes sont requis. Pour permettre aux serveurs d'arrière-plan et de secours d'accéder à ces fichiers, un emplacement partagé est requis. Les installations sous Linux et UNIX peuvent utiliser des montages NFS. La prise en charge d'UNC a été ajoutée pour les installations sous Windows.

- Les performances CA SDM doivent demeurer identiques, même avec les serveurs supplémentaires effectuant des opérations d'arrière-plan et de secours. Si vous déployez davantage de serveurs d'applications, les performances s'amélioreront probablement.
- Chacun des serveurs est directement relié à la base de données, ce qui entraîne une augmentation de la contention des ressources au niveau du SGBD. Nous recommandons d'améliorer la configuration matérielle du serveur de SGBD. Pour de plus amples renseignements, vérifiez les données systèmes.
- La conversion d'une configuration conventionnelle en configuration de disponibilité avancée implique une opération manuelle. Les mises en oeuvre plus volumineuses sont généralement plus complexes et vous pourriez avoir besoin de solliciter CA Services pour obtenir une assistance.
- Pour effectuer une migration vers la configuration de disponibilité avancée, effectuez une mise à niveau vers CA SDM r12.9 dans la configuration conventionnelle, puis effectuez la conversion vers la disponibilité avancée.
- Installez les serveurs d'arrière-plan et de secours sur le même sous-réseau pour obtenir des temps de commande ping et des latences similaires à partir des différents serveurs d'applications.
- Prévoyez de placer les serveurs d'arrière-plan et de secours dans un emplacement central disposant d'une connectivité réseau performante pour tous vos utilisateurs. Vous pouvez placer les serveurs d'applications de manière centrale ou les répartir dans diverses régions.
- Une configuration de disponibilité avancée doit toujours disposer d'un serveur d'arrière-plan et d'au moins un serveur de secours.
  - (Recommandé) Veillez à ce que la configuration du serveur d'arrière-plan et de tous les autres serveurs de secours soit identique. Ce processus permet au serveur de secours de fonctionner comme le serveur d'arrière-plan lors d'un basculement.
  - Vous pouvez configurer autant de serveurs de secours que vous voulez. Pour améliorer la disponibilité CA SDM, prévoyez de placer un serveur de secours dans votre centre de données de sauvegarde ou sur le site de récupération après sinistre.
  - La mise en oeuvre de la disponibilité avancée minimale requiert un serveur d'applications. Nous vous recommandons de disposer de deux serveurs d'applications pour améliorer la disponibilité et d'un équilibreur de charge pour diriger le trafic Web.
  - Mis à part les administrateurs CA SDM, aucun autre utilisateur n'est autorisé à se connecter au serveur d'arrière-plan. De même, aucun utilisateur n'a le droit de se connecter aux serveurs de secours.

- Nous pouvons envoyer des notifications par courriel à partir de tous les serveurs CA SDM. Il n'existe actuellement aucune façon de limiter ou de configurer cette option. Dans la configuration de disponibilité avancée, chaque serveur doit avoir une connexion au serveur de courriel.
  - Une notification par courriel résultat de l'interaction de l'utilisateur final est envoyée à partir du serveur d'applications auquel l'utilisateur est connecté.
  - Une notification par courriel résultant de tout processus d'arrière-plan (comme lorsque Animator effectue le traitement d'un événement joint) est envoyée par l'utilitaire pdm_mail_nxd exécutée sur le serveur en arrière-plan.
  - Lors d'une panne du serveur d'arrière-plan, les courriels mis en file d'attente seront envoyés lorsque le serveur d'arrière-plan deviendra serveur de secours.

Remarques sur le basculement

Dans le cas d'un basculement du serveur d'arrière-plan vers le serveur de secours, tenez compte des remarques suivantes :

- Les nouveaux utilisateurs ne peuvent pas se connecter.
- Pour les utilisateurs déjà connectés, les actions suivantes sont inopérantes pendant le basculement. Elles doivent donc être retentées après le basculement :
  - Création de billets avec des pièces jointes
  - Téléchargement de pièces jointes
  - Recherche de documents de connaissances
  - Indexation de nouveaux documents de connaissances
  - Courriel entrant
  - Événements de SLA qui ne sont pas déclenchés avant la fin du basculement
    - **Important :** Si vous avez configuré votre outil tiers pour activer le basculement automatique des serveurs CA SDM, vous devez le désactiver avant de commencer la maintenance progressive.

Remarques sur la base de données

- Il existe une connexion directe d'un serveur à l'autre ainsi qu'à la base de données. Si le serveur CA SDM se trouve dans la zone démilitarisée (DMZ), vous devez ouvrir les ports de pare-feu ou mettre en oeuvre une technologie de mandataire pour cette connectivité. De même, prévoyez des accords de licence avec votre fournisseur de SGBD.
- Veillez à installer le client de base de données sur tous les serveurs CA SDM.

- Dans la configuration de disponibilité avancée, tous les serveurs se connectent toujours à une seule base de données. Étant donné que la base de données peut constituer un point de défaillance unique, tenez compte des avantages de la mise en grappe de base de données pour augmenter la disponibilité du SGBD.
- Microsoft SQL Server est pris en charge uniquement en mode natif sur la plate-forme Windows. Par exemple, si votre mise en oeuvre comprend des serveurs avec des systèmes d'exploitation hétérogènes tels que Windows et Linux, sélectionnez Oracle comme SGBD, car Microsoft SQL Server n'est pas pris en charge sous Linux.
- L'utilitaire pdm_isql ne peut être utilisé que sur le serveur d'applications.

Configuration, administration et fonctionnement du système

- Les services Web SOAP et RESTful sont uniquement pris en charge sur les serveurs d'applications. Vous pouvez configurer des directeurs Web sur tous les serveurs CA SDM.
- Les serveurs d'applications étant indépendants les uns des autres, les directeurs Web peuvent uniquement traiter des moteurs Web exécutés sur le même serveur d'applications. Les directeurs Web ne peuvent pas traiter les moteurs Web exécutés sur divers serveurs d'applications.
- Étant donné que les serveurs inclus dans la configuration de disponibilité avancée disposent d'un degré d'indépendance supérieur, la plupart des utilitaires de ligne de commande fonctionnent uniquement sur le serveur local. Par exemple, pdm_status affiche uniquement les processus CA SDM exécutés sur le serveur sur lequel vous exécutez la commande. L'utilitaire pdm_webcache actualise uniquement les caches de formulaires sur le serveur sur lequel il a été émis.
- Contrairement à la configuration conventionnelle, dans laquelle vous démarrez et arrêtez les processus CA SDM en exécutant pdm_d_mgr sur le serveur principal, dans la disponibilité avancée, les processus de chaque serveur sont gérés de façon indépendante.
- Il est recommandé d'utiliser la nouvelle commande pdm_server_control au lieu de la commande pdm_halt pour arrêter des serveurs d'applications. Avant l'arrêt, vous pouvez demander aux utilisateurs actifs de passer à un autre serveur d'applications. Pour ce faire, vous pouvez notifier les utilisateurs à l'aide de l'option de mise au repos.
- L'utilitaire pdm_edit a été remplacé par une nouvelle interface utilisateur graphique, éliminant ainsi de nombreux changements manuels du fichier de configuration précédemment requis.

- Contrairement à la configuration conventionnelle, dans la configuration de disponibilité avancée, vous pouvez utiliser l'option bopauth_host du gestionnaire d'options de l'interface utilisateur Web du serveur d'arrière-plan pour préciser les détails du serveur d'authentification. Ce changement de configuration n'est plus effectué dans pdm_edit pour la configuration de disponibilité avancée. Les utilisateurs ne peuvent pas se connecter lorsque le serveur d'authentification est indisponible.

  Remarque : Dans la configuration conventionnelle, vous pouvez utiliser un serveur secondaire pour intégrer CA SDM à un système d'authentification exécuté sur un système différent, voire sur une plate-forme matérielle différente.

- Pour empêcher des serveurs non autorisés d'intégrer la configuration de disponibilité avancée, tous les serveurs doivent être définis dans l'interface graphique du serveur d'arrière-plan avant leur configuration.

- Vous pouvez changer le rôle et d'autres renseignements concernant un serveur dans la configuration de disponibilité avancée sous l'onglet Administration. Avant toute tentative de changement d'une définition de serveur, arrêtez les services CA SDM. Pour que les changements prennent effet, vous devez reconfigurer le serveur.

- Pour permuter entre configuration conventionnelle et configuration de disponibilité avancée pour un serveur, exécutez l'utilitaire de configuration. Veillez à changer tous les serveurs impliqués dans la mise en oeuvre. Vos données restent inchangées, mais les mises à jour manuelles sont requises pour changer les paramètres.

- Utilisez les derniers fichiers pdm_startup lors de la migration vers CA SDM r12.9. N'utilisez pas les fichiers issus de versions précédentes de CA SDM (par exemple : fichiers générés par l'utilitaire pdm_edit).

- De nouvelles variables d'environnement ont été ajoutées à NX.env pour prendre en charge la disponibilité avancée, et le système conserve automatiquement les valeurs variables.

  Important : Ne changez pas NX.env manuellement, sauf indication contraire.

- Une nouvelle fonctionnalité génère des numéros de billet et des clés d'enregistrement numériques. Pour éviter un potentiel endommagement de la base de données, évitez toute tentative de chargement ou de changement manuel de la table Key_Control.
- Vous ne pouvez pas déplacer les démons d'outils de connaissances vers un autre serveur dans la configuration de disponibilité avancée. kt_daemon est désormais exécuté sur tous les serveurs. Tous les autres démons d'outils de connaissances sont exécutés comme singletons sur le serveur d'arrière-plan.
- Les outils de connaissances prennent désormais en charge les chemins d'accès au fichier UNC sous Windows pour l'emplacement des fichiers d'index EBR et les fichiers d'entrée/ de sortie utilisés par la fonctionnalité d'exportation/d'importation de connaissances. Cette fonctionnalité est disponible pour les configurations de disponibilité avancée et conventionnelle.

  Important : Le chemin d'accès aux fichiers d'index EBR et le chemin d'accès aux fichiers KEIT doivent faire référence aux mêmes informations d'authentification UNC et le chemin d'accès doit résider sur le même serveur pour permettre leur prise en charge.
- Le contrôle de version distribue les fichiers (par exemple, htmpl, .maj, .mod et .sch) qui sont configurés dans le fichier server_secondary_custom.ver à partir du serveur d'arrière-plan. Lors du démarrage, le serveur de secours ou d'applications exécute le client de contrôle de version pour obtenir des fichiers mis à jour à partir du serveur d'arrière-plan.
- La fonctionnalité d'archivage/purge est exécutée sur le serveur d'arrière-plan et prend en charge les chemins d'accès au fichier UNC sous Windows pour les fichiers de sortie. Cette fonctionnalité est disponible pour les configurations de disponibilité avancée et conventionnelle.
- Les pièces jointes des courriels entrants sont désormais stockées par pdm_maileater lorsque le référentiel se trouve sur un serveur distant.
- Veillez à permettre au gestionnaire de démons de modifier les procsets et n'exécutez pas la commande pdm_dmnmode pour cette action.

Remarques générales sur l'interface utilisateur Web

- Un serveur Web est requis sur tous les serveurs de la configuration de disponibilité avancée.
- Lorsque le serveur d'arrière-plan n'est pas disponible en raison du basculement, un formulaire Réponse de serveur en retard est proposé aux utilisateurs Web. Les utilisateurs peuvent reprendre leur travail lorsque le serveur de secours remplace le serveur d'arrière-plan.
- La valeur de l'option web_cgi_url doit pointer vers les éléments suivants :
  - L'équilibreur de charge, si vous disposez de plusieurs serveurs d'applications.
  - Le serveur d'applications, si vous en avez un seul.

Remarques sur les pièces jointes

- Vous pouvez améliorer la disponibilité des pièces jointes en configurant plusieurs processus de référentiel de documents et accéder à un référentiel de fichier partagé.

Remarques sur l'outil de conception Web

- Vous ne pouvez utiliser l'outil de conception Web que sur le serveur d'arrière-plan.
- Suivez la procédure recommandée pour publier des changements appliqués aux formulaires de l'outil de conception Web, afin que les formulaires mis à jour soient diffusés à tous les serveurs de l'installation. Pour de plus amples renseignements, reportez-vous à *Comment personnaliser les schémas avec l'outil de conception Web* et *Comment personnaliser l'interface Web avec les scénarios de l'outil de conception Web*.
- Les démons de couche de base de données virtuelle sont exécutés sur tous les serveurs. Installez les personnalisations de base de données CA SDM et les définitions d'objets sur tous les serveurs.

Remarques relatives au signalement

- CA Business Intelligence peut récupérer automatiquement les données auprès d'autres serveurs d'applications. Vous pouvez configurer cette fonctionnalité pour améliorer la disponibilité de la fonction de signalement CA SDM.
- BOXI n'est pas intégré au serveur d'arrière-plan. C'est pourquoi vous ne pouvez pas afficher les rapports à partir de l'interface utilisateur Web du serveur d'arrière-plan. Si vous sélectionnez l'onglet Rapports dans l'interface utilisateur Web du serveur d'arrière-plan, un message d'erreur s'affiche.

Remarques sur le gestionnaire d'options

- Vous pouvez installer ou désinstaller des options par l'entremise du gestionnaire d'options uniquement dans l'interface utilisateur Web du serveur d'arrière-plan. Utilisez la procédure de maintenance progressive pour propager les changements vers tous les serveurs de la configuration. Pour plus de détails sur l'exécution de la procédure de maintenance progressive, consultez la section *Opération de maintenance progressive* dans le scénario intitulé CA SDM.

Remarques sur les services Web

- Vous pouvez configurer des services Web uniquement sur les serveurs d'applications.
- L'option webservices_domsrvr a été supprimée du gestionnaire d'options. Vous pouvez configurer la variable NX_WEBSERVICES_DOMSRVR de manière indépendante sur chaque serveur d'applications en modifiant NX.env.

Remarques générales sur l'intégration

- L'URL vers l'interface utilisateur Web de CA SDM doit pointer vers un serveur d'applications correctement configuré. ca_application_registration contient une URL pointant vers votre installation de CA SDM utilisée par d'autres produits CA. Cette URL pointe vers le premier serveur CA SDM configuré; il s'agit en général du serveur d'arrière-plan. Seuls les administrateurs de CA SDM peuvent changer la valeur à l'aide de la fonctionnalité Administration. Si vous utilisez un équilibreur de charge, pointez cette URL vers celui-ci, au lieu d'un serveur d'applications unique. Pour de plus amples renseignements, consultez l'*Aide en ligne*.
- L'interaction de la plupart des utilisateurs finals et les intégrations à d'autres produits logiciels ont lieu au niveau du serveur d'applications. Aucun basculement n'est prévu pour les serveurs d'application. En cas d'indisponibilité du serveur d'applications, ses services Web seront également indisponibles. Pour améliorer la disponibilité du serveur d'applications, vous pouvez déployer un équilibreur de charge pour router les demandes parmi différents serveurs d'applications.
- Vous pouvez intégrer NSM à un seul serveur d'applications, car les adresses IP sont impliquées. L'intégration de NSM est indisponible lorsque ce serveur est arrêté.
- CA Workflow doit être installé sur l'un des serveurs d'applications. Si ce serveur d'applications tombe en panne, l'intégration de CA Workflow n'est plus disponible.

Remarques sur la conversion

- Vous pouvez uniquement convertir le serveur d'arrière-plan en serveur principal.
- Vous pouvez uniquement convertir le serveur principal en serveur d'arrière-plan.
- Vous pouvez uniquement convertir le serveur secondaire en serveur de secours ou en serveur d'applications.
- Vous pouvez uniquement convertir le serveur de secours ou d'applications en serveur secondaire.

Remarques sur la recherche fédérée

- Pour activer et utiliser la fonction de recherche fédérée, sélectionnez cette option lors de la configuration des serveurs d'applications.

Planification de l'installation de CA MDB

Pour installer et configurer CA MDB, utilisez les renseignements suivants pour rechercher et collecter des données.

- **Recherche** : lisez la *Présentation de CA Management Database* pour vous familiariser avec CA MDB, déterminer votre stratégie de déploiement et consulter les questions relatives à SQL Server ou Oracle dont vous pourriez avoir besoin pour utiliser CA MDB avec CA SDM.
- **SQL Server** :Pour vous assurer que vous pouvez configurer le produit et les composants sur SQL Server, effectuez les opérations suivantes :
  - Activez le protocole TCP/IP sur l'ordinateur sur lequel vous souhaitez effectuer l'installation et la configuration.
  - Ayez les renseignements suivants à disposition :
    - Le nom de l'instance du serveur qui exécute SQL Server.
    - Le nom d'utilisateur et le mot de passe de la base de données SQL Server.
    - Le numéro de port de la base de données SQL Server.
- **Oracle** : Ayez les renseignements suivants à disposition :
  - La base de données Oracle est-elle locale ou distante ?
  - Avez-vous besoin de créer des espaces disque logiques ?
  - Le nom du service Net
  - Le nom et le mot de passe de l'utilisateur DBA.
  - Le nom d'espace disque logique de l'index et des données.
  - Le chemin d'accès complet de l'espace disque logique.
  - Les données de connexion JDBC, y compris l'identificateur de système (SID) et le port d'écoute.

  Remarque : Si vous ne savez pas quelles données entrer pour votre base de données, reportez-vous à l'*Aide en ligne relative à la configuration du serveur*.

Renseignements supplémentaires :

Installation de la CA MDB (page 155)

Remarques relatives à CA MDB

Avant d'installer CA MDB, considérez les informations suivantes pour assurer une mise en oeuvre réussie :

- **AIX** : sur certains ordinateurs AIX, l'espace disponible maximal de la liste ARG/ENV est insuffisant pour pouvoir installer CA MDB. Dans ce cas, lancez la commande *lsattr -lsys0 -ancargs -Fvalue* pour trouver le paramètre actuel de la taille maximale de la liste ARG/ENV. Si la valeur renvoyée est inférieure à 50, augmentez-la au moyen de la commande *chdev -l sys0 -a ncargs=50.*
- **Oracle** : tenez compte des renseignements suivants :
  - Effectuez une sauvegarde de Oracle avant d'appliquer un correctif de CA MDB. La sauvegarde peut être effectuée par un administrateur de base de données ou par le script de correctif. Le script de correctif utilise le gestionnaire de récupération d'Oracle (RMAN) pour sauvegarder la base de données à l'aide de l'authentification de système d'exploitation. La configuration RMAN risque de requérir l'activation de la journalisation des archives (mode ARCHIVELOG) dans la base de données. Si l'administrateur de base de données a effectué la sauvegarde, vous pouvez aussi supprimer la sauvegarde avec le script de correctif en indiquant Non dans le paramètre -ORA_BACKUP.

    Remarque : L'application de correctifs utilise la commande RMAN et l'authentification du système d'exploitation.
  - L'utilisateur Oracle qui est utilisé pour exécuter l'installation de la CA MDB doit disposer des droits d'administrateur de base de données suivants :
    - Rôle dba (connecte sys en tant que sysdba; accorde dba à installation_user;)
    - Rôle sysdba (connecte sys en tant que sysdba et accorde sysdba à installation_user)
    - La capacité à accorder des droits à l'utilisateur mdbadmin pour différentes tables et vues du système (connect sys as sysdba; grant all privileges on "sys". <TABLE_NAME> à installation_user avec l'option d'octroi) Les valeurs considérées par TABLE_NAME sont les suivantes : COL$, DBA_CONSTRAINTS, DBA_CONS_COLUMNS, DBA_INDEXES, DBA_IND_COLUMNS, DBA_OBJECTS, DBA_OBJECT_TABLES, DBA_REGISTRY, DBA_TABLES, DBA_TABLESPACES, DBA_TAB_COLUMNS, DBA_TAB_PRIVS, DBA_VIEWS, DBMS_REGISTRY, EXPDEPACT$, EXPDEPOBJ$, EXPPKGACT$, EXPPKGOBJ$, KOPM$, OBJ$, TS$, USER$

- **Clients distants (UNIX et Linux)** : lorsque la CA MDB est créée à partir d'un client distant, le processus de création de CA MDB se termine avec un code de retour 95 et un message d'erreur dans le journal d'installation indiquant que la *création de l'espace disque logique a échoué*, sauf si le répertoire indiqué dans le chemin d'accès à l'espace disque logique existe à la fois sur l'ordinateur du client et sur le serveur Oracle.
- **Installation des composants de la CA MDB (SQL)** : L'interface du programme d'installation des composants de CA MDB affiche un champ Nom du serveur de la base de données. Ce champ identifie le nom du serveur local ou le nom du noeud de grappe, le cas échéant. Utilisez le nom de réseau qui est utilisé pour la connexion au serveur SQL.
- **Caractères spéciaux (UNIX, Linux et Windows)** : tenez compte des informations suivantes :
  - (UNIX et Linux) L'ID d'utilisateur de l'administrateur de la base de données utilisé pour créer la CA MDB ne peut pas comprendre de caractères spéciaux. En outre, les restrictions suivantes s'appliquent :
    - Le nom d'utilisateur de l'administrateur de la base de données et le nom d'espace disque logique prennent en charge les caractères spéciaux # et _. Tous les autres caractères spéciaux ne sont pas pris en charge.
    - Le mot de passe de l'administrateur de la base de données et le mot de passe MDBADMIN prennent en charge les caractères spéciaux ~, #, %, ^, -, +, _, {, }, [,], :, . et ? Tous les autres caractères spéciaux ne sont pas pris en charge.
    - Le chemin d'espace disque logique Oracle, le répertoire cible de MDB, le répertoire source de MDB et le répertoire DIR de correctifs de MDB prennent en charge les caractères spéciaux ~, %, ^, _, -, +, [,], {, }, :, (y compris <espace> si le chemin d'accès est entre guillemets doubles ; cependant, les espaces consécutifs ne sont pas pris en charge).
  - (Windows) L'ID d'utilisateur de l'administrateur de la base de données utilisé pour créer la CA MDB ne peut *pas* comprendre de caractères spéciaux. En outre, les restrictions suivantes s'appliquent :
    - Le nom d'utilisateur DBA et le nom d'espace disque logique prennent en charge les caractères #, $ et _. Tous les autres caractères spéciaux ne sont pas pris en charge.
    - Le mot de passe DBA et le mot de passe MDBADMIN prennent en charge les caractères spéciaux ~, !, #, $, *, (), _, +, `, -, {}, [], \, :, ', ?, ., / et @. Tous les autres caractères spéciaux ne sont pas pris en charge.
    - Le chemin d'accès de l'espace disque logique Oracle, le répertoire cible de MDB, le répertoire source de MDB et le répertoire de correctifs de MDB prennent en charge les caractères spéciaux ~, !, #, $, (), _, +,`, -, {} et [] (y compris <espace> si le chemin d'accès est entre guillemets doubles).

- **Espaces disque logiques** : tenez compte des informations suivantes :
  - La <msb> utilise l'espace disque logique temporaire du système pour stocker les tables temporaires. Un minimum de 50 Mo d'espace disponible est nécessaire pour cette opération. Si vous décidez d'utiliser des espaces disque logiques existants pour CA MDB, ceux-ci nécessitent alors au moins 200 Mo d'espace disque disponible. Si cet espace n'est pas disponible, la création de la CA MDB ne pourra pas aboutir.
  - Si le processus de création de la CA MDB est utilisé pour créer des données ou indexer un espace disque logique et que le paramètre de taille n'est pas numérique, un code de retour de 350 se produira et le journal d'installation de la CA MDB inclura une erreur (cr=189) indiquant que le processus de création de l'espace disque logique a échoué.
- **Utilisateurs et droits d'administrateur** : si le processus de création de la CA MDB est effectué avec un utilisateur ne disposant pas de droits d'administrateur, il échoue. Le journal d'installation de CA MDB affiche alors l'erreur *ORA-00942 : la table ou la vue n'existe pas*.

Renseignements supplémentaires :

Installation de la CA MDB (page 155)

Planification de l'installation de CA SDM

Pour installer et configurer CA SDM, utilisez les renseignements suivants pour rechercher et collecter des données.

- **Autorisations de connexion** : effectuez les opérations suivantes :
  - (Windows) Connectez-vous en tant qu'administrateur et disposez des autorisations d'administration complètes.
  - (UNIX) Connectez-vous en tant qu'administrateur et disposez des autorisations correctes pour le compte root.
- **Recherche** : effectuez les opérations suivantes :
  - Consultez les Notes de parution *et* le fichier Readme facultatif (si disponible). Ne démarrez pas votre installation tant que vous n'avez pas lu et compris ces informations.

    Remarque : Vous trouverez la version la plus récente des Notes de parution, qui contiennent la configuration système requise, ainsi que le fichier Readme facultatif (si disponible) à l'adresse http://www.ca.com/worldwide.

- Vérifiez que vous avez vos supports d'installation.

  Remarque : Si votre ordinateur ne dispose pas d'un lecteur approprié pour le support d'installation, copiez le contenu du support sur l'ordinateur sur lequel vous souhaitez installer CA SDM. Puis, démarrez l'installation. Pour une installation distante sur un réseau, il se peut que vous deviez partager un lecteur ou un dossier sur le réseau et vous y connecter pour démarrer l'installation.

  Important : N'installez pas les DVD d'installation de CA SDM sur un système d'exploitation Windows XP, car certains des fichiers d'installation seront introuvables et l'installation échouera.

- Consultez la matrice de certification pour connaître la liste de logiciels tiers qui ont été certifiés pour être utilisés avec CA SDM.

  Remarque : Vous trouverez la version la plus récente de la matrice de certification à l'adresse http://www.ca.com/worldwide.

- Renseignez-vous sur les composants du produit et veillez à en comprendre les bases.

- Familiarisez-vous avec les différents types de stratégies de mise en oeuvre prises en charge par le produit. Tenez compte de la disponibilité, de la bande passante utilisable et de la capacité de réaction du réseau lorsque vous décidez de la meilleure stratégie de mise en oeuvre pour votre organisation.

- Consultez les remarques concernant la mise en oeuvre pour chaque composant que vous installez.

- **Répertoire de base d'installation** : effectuez les opérations suivantes :
  - Déterminez le répertoire de base dans lequel vous voulez installer le produit. Le répertoire de base par défaut du produit est C:\Program Files\CA\Service Desk Manager.
  - Déterminez le répertoire de base dans lequel vous voulez installer les composants partagés que le produit utilise (par exemple, l'environnement d'exécution Java (JRE) et Apache Tomcat). Le répertoire de base par défaut pour les composants partagés est C:\Program Files\CA\SC.
- **Base de données** : choisissez la base de données (SQL Server ou Oracle) à utiliser avec CA SDM et installez-la. Ensuite, effectuez les opérations suivantes :
  - **SQL Server** : Activez le protocole TCP/IP sur l'ordinateur sur lequel vous souhaitez effectuer l'installation et la configuration.

- **Serveur principal, serveurs secondaires et configuration de l'utilisateur** : effectuez les opérations suivantes :
  - Pour garantir que vous pouvez configurer aussi bien le serveur principal que les deux serveurs secondaires facultatifs à la fin de l'installation du produit, munissez-vous des renseignements suivants :
    - Le système de noms de domaine (DNS) des serveurs principal et secondaires.
    - Le nom ou l'alias du serveur.
    - Le nom ou les alias du gestionnaire d'objets auquel vous voulez établir une connexion.
    - Le nom ou l'adresse IP du serveur secondaire.
    - Le port de connecteur logiciel slump que l'ensemble de CA SDM doit utiliser pour communiquer.
    - Le port de connecteur logiciel de l'utilitaire de surveillance que le serveur secondaire doit utiliser pour écouter les messages du serveur principal.
  - Pour garantir que vous pouvez configurer les données de compte pour l'administration du produit à la fin de son installation, munissez-vous d'un nom d'utilisateur et d'un mot de passe à forts privilèges et restreint.
  - (UNIX et Linux) Créez manuellement votre utilisateur à forts privilèges. Sous Windows, cet utilisateur est automatiquement créé pendant la configuration du produit, mais sous UNIX et Linux, vous devez le créer manuellement.

Remarque : Pour configurer le serveur de disponibilité avancée, consultez le scénario Configuration des serveurs pour la disponibilité avancée.

- **Configuration de l'interface Web** : effectuez les opérations suivantes :
  - Pour garantir que vous pouvez configurer l'interface Web à la fin de l'installation du produit, munissez-vous des renseignements suivants :
    - Le nom de l'hôte Web et le serveur Web.
    - (Windows NT uniquement) Le site Web devant être utilisé par le serveur CA SDM.
    - Le numéro de port Tomcat et le numéro de port de connecteur logiciel pour des demandes d'arrêt.
- **Navigateurs et logiciels antivirus** : effectuez les opérations suivantes :
  - (Firefox) Activez facultativement l'authentification Windows (authentification unique d'entreprise).
  - Désactivez temporairement tout logiciel antivirus, car cela ralentit l'installation. Après l'installation, assurez-vous d'activer votre logiciel antivirus à nouveau.

- **Outil de conception Web** : L'Outil de conception Web s'installe automatiquement sur le serveur principal quand vous installez CA SDM. Vous pouvez installer l'Outil de conception Web sur des ordinateurs distincts à l'aide des supports d'installation.
- **Création de noms de fichiers** : CA SDM requiert la création de noms de fichiers 8.3. Reportez-vous à la documentation de soutien et à l'Aide de votre système d'exploitation pour de plus amples renseignements sur la création de noms de fichiers au format 8.3 et sur l'entrée de registre disable8dot3.

Remarques relatives à CA SDM

Avant d'installer CA SDM, considérez les renseignements suivants pour assurer une mise en oeuvre réussie :

- **Serveur Apache (UNIX et Linux)** : Si vous utilisez le serveur Apache sous UNIX ou Linux, certaines installations du serveur Apache désactivent l'OPTION FollowSymLinks du répertoire racine. Cette option désactive l'intégration par défaut d'Apache pour CA SDM, car le fichier de configuration utilise le lien symbolique /opt/CAisd créé pendant l'installation de CA SDM. Pour utiliser CA SDM avec Apache, activez l'option FollowSymLinks à partir du répertoire racine (fichier httpd.conf) ou modifiez le fichier $NX_ROOT/bopcfg/www/CAisd_apache.conf pour remplacer le lien symbolique par le chemin d'accès utilisé. Dans le fichier CAisd_apache.conf, remplacez toutes les occurrences de /opt/CAisd par l'emplacement de CA SDM (par exemple, /opt/CA/ServiceDeskManager). Une fois la modification effectuée et enregistrée, arrêtez le serveur Apache et redémarrez-le pour appliquer la modification.
- **Navigateurs** : tenez compte des renseignements suivants :
  - (Firefox) Tenez compte des renseignements ci-après :
    - Il se peut qu'une erreur de type *Script sans privilèges* surviennent lorsque vous utilisez les fonctionnalités Couper, Copier et Coller sur la page de l'éditeur HTML dans les Catégories de connaissances. Cliquez sur OK pour visualiser une note technique sur mozilla.org décrivant comment autoriser un script à accéder au presse-papiers.
    - Lorsque vous affichez le contenu d'un fichier joint dont le nom contient des caractères de type Latin-1 étendu, la boîte de dialogue Enregistrer sous s'affiche. Vous pouvez enregistrer le fichier ou cliquer sur Ouvrir et sélectionner une application pour ouvrir la pièce jointe.
  - (Internet Explorer 8 sous Windows 2008) Si le niveau de sécurité Internet est défini sur élevé, l'URL de CA SDM et le site *about:blank* doivent être ajoutés aux sites de confiance des pages Web pour être affichés correctement.

- (Barre d'outils Google) L'interface Web de CA SDM risque de ne pas afficher correctement le texte de la barre de titre en haut de la fenêtre.
- (Internet Explorer 8.0) Il se peut que la mémoire utilisée soit parfois augmentée lors de l'accès à l'interface Web de CA SDM. Il s'agit d'un problème connu de la version actuelle d'Internet Explorer. Pour libérer de la mémoire, réduisez régulièrement la page Web de CA SDM.

- **CA Workflow** : tenez compte des renseignements suivants :
  - Si l'information d'authentification de l'utilisateur à forts privilèges est incorrecte lors de la configuration, CA SDM peut s'exécuter mais CA Workflow ne fonctionne pas. Si cette information est erronée, les problèmes suivants risquent de survenir :
    - CA Workflow ne s'installe pas Un message d'erreur indiquant un nom ou un mot de passe utilisateur incorrects apparaît dans le fichier /site/Workflow/wekinstall.log.
    - Tomcat consomme trop de ressources de l'UC et/ou le fichier journal /log/pdm_tomcat.log est rempli d'exceptions du gestionnaire de sécurité et de messages du type *AbandonedObjectPool is used*.

    Pour résoudre ce problème, vérifiez le nom et le mot de passe de l'utilisateur à forts privilèges en vous connectant avec ces derniers au système d'exploitation. Exécutez ensuite la configuration de CA SDM et spécifiez le nom et le mot de passe corrects de l'utilisateur à forts privilèges. Si le mot de passe de l'utilisateur à forts privilèges est modifié, vous devez lancer la configuration pour définir le nouveau mot de passe.
  - Si l'information d'authentification de l'utilisateur à forts privilèges est modifiée après l'installation de CA Workflow, le processus de CA Workflow peut échouer. Effectuez les opérations suivantes :
    a. Connectez-vous à CA Workflow IDE pour modifier l'Acteur de service Web CA SDM par défaut.
    b. Sélectionnez l'onglet Acteurs, développez l'arborescence JavaScript, et cliquez sur USDInitializer.
    c. Double-cliquez sur l'option d'obtention d'attributs globaux.
    d. Sous la section de script, entrez le nom et le mot de passe de l'utilisateur à forts privilèges CA SDM dans les champs suivants :

       USD_Username = ""

       USD_Password = ""
    e. Modifiez ces valeurs dans le fichier $NX_ROOT\data\workflow\actors\r12_Service_Desk_Actors_en_US.xml.

- **Bases de données (toutes prises en charge)** : tenez compte des renseignements suivants :
  - La configuration échouera si CA SDM a été configuré avec une base de données, puis que la configuration est exécutée une deuxième fois et qu'un type différent de base de données est sélectionné. Par exemple, si vous effectuez d'abord une configuration pour SQL Server, puis une autre pour une base de données Oracle. Pour contourner le problème, redémarrez l'ordinateur avant d'exécuter la deuxième configuration.
  - Si les données de connexion à la base de données sont différentes, elles ne seront pas acceptées dans les configurations suivantes. Si une configuration supplémentaire est requise suite à une modification dans les données de connexion à la base de données, supprimez le fichier $NX_ROOT\NX.env avant de poursuivre.
  - Si vous avez mis Argis 8.0 à niveau vers CA Asset Portfolio Management r11.2 et que vous partagez CA MDB (base de données) avec CA SDM, il se peut que vous rencontriez des problèmes lors de la tentative d'ajout ou de mise à jour d'actifs dans les familles d'actifs à l'aide de CA SDM. Pour éviter les erreurs, vous devez définir les tables d'extension d'actif sur CA SDM à l'aide de l'une des méthodes suivantes :
    - Utilisez l'outil de conception Web afin de définir les tables et les formulaires permettant de visualiser et de modifier les entrées de tables.
    - Modifiez manuellement les tables et les formulaires à l'aide des instructions suivantes :

    a. Le fichier $NX_ROOT\bopcfg\majic\assetx.maj contient un modèle qui peut être utilisé pour créer un fichier majic permettant d'identifier les colonnes de la table d'extension des actifs en fonction de l'architecture de CA SDM. Copiez ce fichier et modifiez-le selon vos besoins en suivant les instructions contenues dans ce dernier.

    b. Créez un fichier .sch dans le dossier $NX_ROOT\site\mods afin de définir les colonnes de la base de données. Les fichiers $NX_ROOT\site\assetx_schema.sch et $NX_ROOT\site\assetx_index.sch peuvent être utilisés comme modèles. Vous pouvez les copier et les modifier selon vos besoins pour vos tables d'extension d'actifs.

    Remarque : Le formulaire permettant d'afficher les données d'extension d'actifs est créé à l'aide de l'outil de conception Web.

- **SQL Server** : tenez compte des renseignements suivants :
  - La dernière version de SQL Server dispose d'une information d'authentification plus stricte que ses versions antérieures. Vérifiez que le mot de passe de la base de données CA SDM respecte les politiques de mots de passe définies dans SQL Server. Si le mot de passe de la base de données CA SDM ne respecte pas la politique de mot de passe de SQL Server 2005, la configuration de CA SDM ne fonctionnera pas.
  - (Environnement en grappe Microsoft sur SQL Server 2005) Dans la grappe, vous devez créer un alias pour le nom de noeud virtuel SQL. Ainsi, lorsque la grappe bascule, CA SDM peut toujours se connecter au même nom de serveur, quel que soit le noeud de grappe soit actif.
- **Oracle** : tenez compte des renseignements suivants :
  - Si vous installez CA SDM sur un système UNIX avec une base de données Oracle, l'utilisateur à forts privilèges doit appartenir au groupe spécifié pendant l'installation de Oracle. Le groupe d'installation Oracle se trouve dans le fichier *oraInst.loc*.
  - Lors de la configuration d'une base de données Oracle 64 bits sur un ordinateur 64 bits, le chemin d'accès de la bibliothèque du système (LD_LIBRARY_PATH sous Oracle Solaris, LIBPATH sous AIX) doit pointer vers les bibliothèques Oracle 32 bits. Les bibliothèques Oracle 32 bits se trouvent dans $ORACLE_HOME/lib32. Ceci est valable à la fois pour la configuration et l'exécution.
  - Pour configurer une base de données Oracle 11g 64 bits sur un ordinateur 64 bits, vous *devez* également installer le client Oracle 32 bits sur le serveur. Lors de la configuration de la base de données, le chemin d'accès à la bibliothèque du système (LD_LIBRARY_PATH sur Oracle Solaris et Linux, LIBPATH sur AIX) *doit* pointer vers les bibliothèques Oracle 32 bits. Cette étape est requise à la fois pour la configuration et l'exécution. Créez également un nom de service réseau sur le client Oracle pour pointer vers l'instance de serveur de la base de données Oracle.
  - Avec une base de données Oracle, si vous souhaitez utiliser les espaces disque logiques existants, vous devez créer un espace disque logique de données d'au moins 400 Mo et un espace disque logique d'index d'au moins 100 Mo avant de configurer CA SDM.
- **Lecteurs externes** : lors de l'installation de CA SDM sous Linux avec 20 lecteurs externes ou plus, vous pouvez constater un retard lors de l'installation, entre les pages de l'assistant d'installation et l'affichage de la page de progression de l'installation. Ce comportement est normal et l'installation devrait reprendre après le retard.

- **Install Shield et InstallAnywhere** : tenez compte des renseignements suivants :
  - Si vous recevez un message d'erreur InstallShield lorsque vous tentez d'installer CA SDM, patientez jusqu'à l'arrêt de *msiexec.exe*. Essayez ensuite d'installer le produit.
  - Si vous démarrez l'installation de CA SDM sous UNIX ou Linux et que vous l'arrêtez, il se peut que vous constatiez la présence d'un répertoire à la racine de l'installation nommé *install.dir.#####*. Il s'agit d'une fonctionnalité d'InstallAnywhere. Ces fichiers ne sont pas nécessaires et vous pouvez les supprimer en toute sécurité.
- **Répertoire de base de l'installation** : lors de l'installation de CA SDM, n'installez pas les composants partagés CA dans le même répertoire que le répertoire d'installation de CA SDM (NX_ROOT).
- **International** : tenez compte des renseignements suivants :
  - Vous ne pouvez pas utiliser de caractères multi-octet dans votre nom d'utilisateur actuel ni dans le nom d'un utilisateur à forts privilèges CA SDM lorsque vous effectuez une installation sur des systèmes d'exploitation multi-octet, tels que des systèmes utilisant le chinois simplifié ou le japonais. L'installation échouera si vous ne respectez pas cette règle.
  - Vous ne pouvez pas entrer de caractères multi-octet dans les noms de chemin des fichiers lors de l'installation et de la configuration. L'installation et/ou la configuration échouera si vous ne respectez pas cette règle.
  - CA SDM doit s'exécuter avec des paramètres régionaux UTF-8 sur les plates-formes UNIX et Linux.
  - Les noms Timespan Symbol fournis avec l'installation par défaut de CA SDM (onglet Administration, Centre de services, Données d'application, Codes, Périodes) sont en anglais. Par exemple, TODAY (Aujourd'hui), YESTERDAY (Hier), THIS MONTH (Mois en cours) et ainsi de suite. Pour obtenir des versions localisées du produit, l'administrateur peut définir les nouvelles périodes localisées comme obligatoires. Vous ne devez ni supprimer, ni modifier les périodes par défaut.
  - Dans CA SDM, les formats de date tels que les spécificateurs internationaux (comme JJ/MM/AAAA pour le français) ne sont pas pris en charge. La syntaxe est limitée aux spécificateurs génériques tels que DD/MM/YYYY. Cependant, de nombreux schémas courts internationaux de type date-heure peuvent être créés à partir de ces spécificateurs génériques (par exemple, YYYY.MM.DD correspond au format de date court utilisé pour le japonais).
  - Pour les notifications par courriel sortante au format texte, il se peut que les options NX_SMTP_HEADER_CHARSET et NX_SMTP_BODY_CHARSET doivent être ajustées (directement dans le fichier NX.env) pour marquer correctement le courriel avec le codage de caractères utilisé par l'environnement d'exploitation international afin qu'il soit bien interprété et affiché par le système de messagerie du destinataire. Les valeurs par défaut de ces options sont définies sur UTF-8 sur toutes les plates-formes.

- Pour les installations de Oracle exécutées sous UNIX ou Linux dans une autre langue que l'anglais, vous devez définir la variable de l'environnement NLS_LANG avant d'exécuter pdm_init. L'administrateur de base de données Oracle doit vérifier la documentation Oracle pour connaître la valeur à affecter à NLS_LANG.

  Important : Si vous ne définissez pas la variable NLS_LANG, le client Oracle utilise par défaut la valeur *American_America.US7ASCII*. Par exemple, pour tester le japonais multi-octet dans votre environnement, définissez NLS_LANG sur *JAPANESE_JAPAN.UTF8*.

  Remarque : La variable NLS_LANG doit être définie dans le même interpréteur de commandes avant d'exécuter pdm_init. Par exemple : *setenv NLS_LANG GERMAN_GERMANY.WE8ISO8859P1*.

- Les utilisateurs internationaux peuvent ajuster la propriété DateFormat du fichier web.cfg pour bénéficier des formats de date et de date et heure utilisés dans leur pays.

- Les utilisateurs internationaux peuvent remplacer le lexique du vérificateur orthographique par défaut (option LEX_LANG dans le gestionnaire d'options) par le lexique correspondant à la langue utilisée.

- La version en anglais du serveur CA SDM est certifiée pour être opérationnelle dans 9 environnements d'exploitation linguistiques autres que l'anglais. Pour Windows, ces environnements doivent être des versions totalement localisées des systèmes d'exploitation du serveur Windows pris en charge. En outre, les environnements d'exploitation Windows qui utilisent un pack d'interface de langue ou une MUI (Multilingual User Interface, interface utilisateur multilingue) fonctionnant sur un noyau en anglais ne sont pas pris en charge.

  De plus, les versions localisées de CA SDM ne sont prises en charge que lorsqu'elles fonctionnent dans un environnement d'exploitation de serveur Windows localisé correspondant. Dans tous les cas, l'option Langue pour les programmes non-Unicode du système (page de code ANSI par défaut sous Windows) doit être configurée de façon appropriée dans la fenêtre Options régionales et linguistiques, accessible à partir du Panneau de configuration, pour pouvoir prendre en charge la langue certifiée cible.

  Remarque : Pour de plus amples renseignements sur les versions localisées des systèmes d'exploitation Windows Server, reportez-vous à la liste des systèmes d'exploitation Microsoft localisés sur le portail informatique et de développement global de Microsoft.

- Pour que les recherches de connaissances contenant des caractères japonais multi-octet pour les utilisateurs internationaux de CA SDM et Gestion des connaissances fonctionnent correctement avec SQL Server uniquement quand SQL Server est installé avec le classement de Windows. Vous devez spécifier l'option de classement pour vos données lors de l'installation de SQL Server.

- **IPV4** : en cas d'installation sous Linux, le fichier /etc/hosts doit contenir une entrée IPV4 avec l'adresse IP, le nom d'ordinateur et le nom qualifié complet de l'ordinateur. Exemple d'entrée :

  ```
  127.0.0.1 localhost.localdomain localhost
  141.202.211.11 usbegp11.ca.com  usbegp11
  ```

- **Noms de fichier courts** : si vous avez désactivé les noms de fichier courts sur votre système d'exploitation Windows, activez-les avant d'essayer d'installer CA SDM. Vous devez également définir les variables d'environnement TEMP et TMP au format de nom de fichier court (c:\temp, par exemple) après avoir activé les noms de fichiers courts avant de démarrer le processus d'installation.

  Remarque : Pour de plus amples renseignements, reportez-vous à l'article 121007 de la base de connaissances Microsoft sur le site Web de soutien et d'aide de Microsoft.

- **Caractères spéciaux et espaces (répertoire, chemin du support et nom de dossier)** : tenez compte des renseignements suivants :

  - Si vous copiez le DVD d'installation sur un disque dur local sur des systèmes UNIX ou Linux, le chemin d'accès au dossier ne doit pas contenir d'espace ni de caractère spécial (tel que #). Si l'emplacement contient des espaces ou des caractères spéciaux, l'installation ne fonctionnera pas.
  - (UNIX, Linux et Windows) N'insérez *pas* d'espaces dans le chemin du support d'installation ni dans le nom du dossier d'installation. Si vous le faites, l'installation ne fonctionnera pas.

- **Tomcat** : tenez compte des renseignements suivants :

  - Tomcat est défini comme serveur Web CA SDM par défaut pendant l'installation du produit. Si vous voulez utiliser les IIS (sous Windows) ou Apache (sous UNIX ou Linux) comme serveur Web par défaut, exécutez la configuration et sélectionnez IIS ou Apache lorsque vous y êtes invité, ou exécutez la configuration à nouveau et sélectionnez IIS ou Apache.
  - Si Tomcat est configuré avec l'option d'authentification externe sur le serveur principal, vous devez configurer un serveur secondaire avec un moteur Web et un démon de référentiel afin de permettre aux utilisateurs non authentifiés d'utiliser les pièces jointes. L'installation de Tomcat sur un serveur secondaire ne permet pas d'utiliser l'authentification externe.
  - L'installation de CA SDM définit le port de Tomcat sur 8080. D'autres produits CA tels que CA Asset Portfolio Management ou la suite de produits Service Delivery spécifient également le port 8080 comme port Tomcat par défaut. Si vous installez plusieurs produits CA sur le même serveur, vous devez sélectionner un port autre que le port 8080 pour que les installations suivantes des produits CA Technologies fonctionnent correctement. Pour remplacer le numéro de port de Tomcat par une autre valeur que 8080 pour CA SDM, installez le produit ou s'il a déjà été installé, exécutez à nouveau la configuration du produit et spécifiez un numéro de port disponible pour Tomcat lorsque vous y êtes invité.

- Il se peut qu'après un redémarrage, le processus Tomcat de CA SDM ne s'exécute pas correctement. Dans ce cas, arrêtez et relancez TOMCAT en utilisant les commandes suivantes :

  ```
  pdm_tomcat_nxd –c stop
  pdm_tomcat_nxd –c start
  ```

- **Utilisateurs et authentification** : tenez compte des renseignements suivants :
  - L'authentification de l'utilisateur ne fonctionnera pas si le système utilise des fichiers en double et si le champ de mot de passe du fichier /etc/passwd comporte la lettre *x*.
  - Sur les systèmes HP, si vous avez configuré la sécurité pour que les mots de passe système soient stockés dans /etc/shadow (par exemple, un *x* est stocké dans /etc/passwd au lieu des mots de passe), l'authentification de l'utilisateur de CA SDM échouera et les utilisateurs ne pourront pas se connecter à CA SDM.
  - Le mot de passe spécifié pour l'utilisateur à forts privilèges doit être conforme aux politiques de mot de passe imposées par le domaine du réseau. S'il ne répond pas aux contraintes imposées par le domaine, la configuration de CA SDM ne fonctionnera pas.
- **Interface Web et Internet Information Services (IIS)** : Pour configurer l'interface Web avec IIS 7.0 sous Windows 2008, vous devez installer les composant CGI et Metabase Compatibility d'IIS 7.0. Vous pouvez ajouter ces composants à l'aide de la section Rôles du gestionnaire de serveur, en installant les modules de compatibilité de gestion d'IIS.
- **Outil de conception Web** : tenez compte des renseignements suivants :
  - Quand vous installez l'outil de conception Web dans le cadre de l'installation de CA SDM, il doit être configuré pour fonctionner correctement.
  - Dans une session d'aperçu de l'Outil de conception Web en mode test, les filtres de recherche sont ignorés sur les nouvelles tables qui ne sont pas publiées.

Renseignements supplémentaires :

Installation de CA SDM (page 163)

Composants de la CA CMDB

CA CMDB fournit les composants standard suivants :

Pages d'interface Web de la CA CMDB

- Définit et assure le suivi des propriétés des CI et de leurs relations entre eux.
- Prend en charge l'impact des modifications et l'analyse des causes premières.

Visualiseur CA CMDB

- Traduit graphiquement les relations entre les CI.
- Prend en charge la fonction de planification.

Contrôle de version

- Affiche l'historique des modifications des CI et leurs relations.
- Compare les instantanés et les jalons nommés.

Visionneuse d'actifs communs

- Affiche simultanément les attributs d'actifs de différents produits
- Constitue le point de lancement des produits de prise en charge.

Rapprochement des CI

- Associe les données de CI importés aux CI existants dans la CMDB.
- Utilise l'API de registre d'actifs existante.

Référentiel

- Constitue un magasin de données pour les CI, les relations, les familles, etc.
- Existe dans la MDB.

Intégration

- Fournit une intégration prédéfinie et standard avec CA Service Desk, CA NSM, CA Asset Portfolio Management, CA EEM et d'autres applications.

Signalement

Fournit les rapports ci-dessous pour les CI.

- Récapitulatif
- Détail
- CI modifiés
- Famille de CI
- Relation de CI
- Arborescence de relations

Remarques sur la planification de Automatisation du soutien

Vous pouvez utiliser les informations suivantes pour rechercher et réunir des renseignements qui vous aideront à planifier une configuration réussie de Automatisation du soutien.

- Lisez les notes de parution pour connaître les conditions requises par Automatisation du soutien.

- **Serveur et réseau** : tenez compte des modes serveur Automatisation du soutien pris en charge suivants :
  - **Serveur principal** : Automatisation du soutien utilise le serveur d'applications principal. Le serveur fournit les communications basées sur un connecteur logiciel et HTTP.
  - **Serveur mandataire de connecteur logiciel** : Automatisation du soutien utilise un mandataire de connecteur logiciel sur le même niveau que le serveur Web qui récupère le traitement du chiffrement/déchiffrement sur le serveur principal pour les connexions de connecteur logiciel directes dans une optique de modularité.
  - **Serveur de routage de messages (MSR)** : Automatisation du soutien isole le trafic imprévisible et requérant beaucoup de bande passante du serveur d'applications principal afin de favoriser la modularité du serveur ; il fournit également un raccourci de routage réseau à l'aide de connexions de contrôle à distance pour assurer la modularité géographique.
- **Dimensionnement du serveur** : tenez compte des variables de serveur ci-dessous.
  - **Caractéristiques réseau des connexions d'utilisateur final et d'analyste** : la charge du serveur est directement proportionnelle aux données du composant de routage des messages. Une bande passante faible, une latence élevée et une perte importante de paquets contribuent à réduire de façon importante la charge sur le serveur. Quand l'état du réseau est optimal (bande passante élevée, faible latence, faible perte de paquets), la vitesse est bien plus élevée sur le réseau. Le nombre total de connexions simultanées d'utilisateurs d'analystes et d'utilisateurs finals par minute, y compris celles d'utilisateurs du libre-service, peut faire peser une lourde charge sur le serveur.
  - **Type de connexion** : le nombre de connexions de connecteur logiciel, à la différence du nombre de connexions HTTP, affecte les serveurs de la façon suivante :
    - Quand vous vous connectez essentiellement à l'aide de connexions de connecteur logiciel, la charge sur les serveurs est si légère que, si le matériel est puissant, l'application dépend du réseau plutôt que de l'ordinateur. Ce n'est pas le matériel mais plutôt le réseau qui peut limiter le nombre de connexions simultanées.
    - Quand vous vous connectez par HTTP, la charge pesant sur les serveurs Web et d'applications est plus importante et l'application dépend de l'ordinateur, à moins qu'elle ne soit fortement mise à l'échelle.

- **Utilisation de Remote Control** : Remote Control utilise une grande quantité de bande passante réseau, de façon soutenue, chaque fois qu'il s'exécute. Tout le trafic acheminé entre les utilisateurs finals et les analystes passe par le serveur. Le nombre de connexions Remote Control simultanées a une influence majeure sur les évaluations de dimensionnement.

  Remarque : Remote Control est le seul outil de large bande passante de l'ensemble d'outils Assistance en direct. Le clavardage et l'automatisation utilisent peu de bande passante. La capture d'écran et le transfert de fichiers peuvent utiliser une large bande passante pendant de courtes périodes de temps, pendant le transfert des fichiers.

Remarques relatives au réseau Automatisation du soutien et à la bande passante

La quantité de bande passante que vous consommez sur l'ordinateur utilisateur final dépend des outils que vous utilisez.

- Les fonctionnalités de clavardage et d'automatisation requièrent peu de bande passante. Un modem à composition automatique de 56 kbps ou moins suffit à prendre ces fonctions en charge.
- En revanche, la fonction Remote Control requiert davantage de bande passante. Cependant, l'assistance en direct de Remote Control s'adapte automatiquement aux environnements à faible bande passante en réduisant la qualité de l'image et la fréquence de rafraîchissement de la session de contrôle à distance.

La quantité de bande passante dépend également du modèle de connexion employé. Deux modèles de connexion sont disponibles.

- La connectivité HTTP s'utilise lorsque l'utilisateur final se trouve derrière un pare-feu restrictif qui n'autorise que les connexions HTTP au serveur.
- Le modèle de connexion de connecteur logiciel directe par SSL s'utilise lorsque l'utilisateur final se connecte au serveur par l'entremise d'une connexion sur le port SSL 443.

Le graphique ci-dessous illustre la quantité de bande passante nécessaire selon les outils que vous utilisez.

Outils/Bande passante	Clavardage/Automatisation	Remote Control
< 3 kbps (28,8 kbps pour l'accès à distance)	Très rapide et réactive	Slow
< 5 kbps (< 56 kbps pour l'accès à distance)	Très rapide et réactive	Adéquat avec dégradation d'image
< 50 kbps (Câble/ADSL)	Très rapide et réactive	Très rapide et réactive
< 100 kbps (LAN)	Très rapide et réactive	Très rapide et réactive

Planification de l'installation de CA NSM

Pour faciliter l'installation et la configuration de CA NSM, lisez la documentation CA NSM, notamment les *Notes de parution* et le fichier Readme facultatif (s'il est disponible).

Planification de l'installation de CA EEM et CA Workflow

Pour vous aider à planifier l'installation et la configuration de CA EEM et CA Workflow, utilisez les renseignements suivants pour rechercher et rassembler des données.

- **Recherche** : effectuez les opérations suivantes :
  - Lisez votre documentation de CA EEM et CA Workflow, y compris les Notes de parution et le fichier Readme facultatif (si disponible).

    Remarque : CA EEM n'est pas une option de configuration dans CA SDM. CA EEM doit être installé séparément.
  - Vérifiez si vous avez une installation CA EEM existante que vous pouvez utiliser avec CA Workflow. Dans ce cas, ne réinstallez *pas* CA EEM. À la place, installez CA Workflow et référencez votre installation CA EEM existante.
  - Notez votre mot de passe d'administration de CA EEM car vous en aurez besoin pendant l'installation.
- **Installation de CA Workflow** : effectuez les opérations suivantes :
  - Avant d'essayer d'installer CA Workflow, assurez-vous d'avoir installé CA EEM. Vous ne pouvez pas installer CA Workflow tant que ce produit n'est pas installé.
  - Si vous voulez utiliser CA Workflow avec CA SDM r12.9, téléchargez d'abord CA SDM r12.7 ISO à partir du Service de soutien de CA, puis installez CA Workflow.
  - Par défaut, le numéro de port Tomcat pour CA SDM est 8080, et 8090 pour CA Workflow. Si ces numéros de port sont déjà utilisés par un autre produit, modifiez les numéros de port de CA SDM et CA Workflow afin d'éviter tout conflit.

- **CA EEM et AIX :** si vous installez CA EEM sous AIX et que vous avez configuré AIX pour Network Information Service (NIS), ajoutez un utilisateur nommé *dsa* avant d'installer CA EEM et CA SDM. Dans ce type de situation, procédez comme suit :

  1. Créez un utilisateur avec l'ID d'utilisateur *dsa*.
  2. Définissez le répertoire de base dsa sur /opt/CA/eTrustDirectory/dxserver. Si les répertoires n'existent pas, créez-les manuellement.

     Remarque : Cette étape n'est obligatoire que pour CA EEM 8.3 et versions antérieures. Le répertoire de base pour CA EEM 8.4 est désormais /opt/CA/Directory/dxserver et est créé automatiquement pendant l'installation.
  3. Veillez à rendre dsa propriétaire de /opt/CA/eTrustDirectory et de tous les sous-répertoires. Pour rendre dsa propriétaire, vous pouvez utiliser une commande similaire à celle qui suit :

     chown -R dsa /opt/CA/eTrustDirectory
  4. Vérifiez l'existence de l'utilisateur, le répertoire de base et la possession de /opt/CA/eTrustDirectory.

Remarques relatives à CA EEM

Avant d'installer CA EEM, considérez les informations suivantes pour assurer une mise en oeuvre réussie :

- **Migration** : lorsque vous effectuez la migration vers CA SDM r12.9, effectuez la mise à niveau vers CA EEM r8.4 SP4 CR05 ou une version ultérieure après l'installation de CA SDM.
- **Magasin de données LDAP externe :** si CA EEM est configuré pour utiliser un magasin de données LDAP externe, l'utilisateur à forts privilèges doit être créé dans l'annuaire LDAP.

  Remarque : Pour de plus amples renseignements sur la configuration du serveur LDAP externe, reportez-vous au *Manuel d'administration*.

Renseignements supplémentaires :

Installation de CA EEM (page 224)

Remarques relatives à CA Workflow

Avant d'installer CA Workflow, considérez les informations suivantes pour assurer une mise en oeuvre réussie :

- CA Workflow est installé sur les serveurs CA SDM suivants, selon votre configuration de CA SDM :
  - Conventionnelle : serveur principal ou secondaire
  - Disponibilité avancée : l'un des serveurs d'applications
- **Nom d'utilisateur ou mot de passe de la CA MDB :** tenez compte des informations suivantes :
  - Si vous modifiez l'utilisateur ou le mot de passe de la base de données CA MDB après l'installation initiale de CA SDM, vous devez réexécuter l'installation de CA Workflow pour que CA Workflow applique les modifications et puisse communiquer avec CA SDM. Lorsque vous réexécutez l'installation de CA Workflow, CA SDM définit automatiquement le nouveau nom et le nouveau mot de passe de l'utilisateur pour CA Workflow et vous ne pourrez *pas* modifier les valeurs manuellement lors de l'installation de CA Workflow.

    Remarque : Les variables d'environnement Oracle doivent être définies avant d'installer CA Workflow sous UNIX et Linux. Si la variable de ORACLE_HOME n'est pas définie, vous obtenez un message d'erreur en cliquant sur le lien d'installation.
  - Si vous migrez vers une nouvelle base de données, exécutez l'utilitaire de migration de flux de travaux (page 120).
- **IPv6** : si votre serveur Linux est configuré pour prendre en charge IPv6, vous ne pourrez peut-être pas vous connecter à l'IDE CA Workflow. Pour résoudre ce problème, modifiez le fichier de script ide.sh situé dans le dossier $NX_ROOT\site\Workflow\Client en modifiant la deuxième ligne "VMARGS =" en "VMARGS=-Djava.net.preferIPv4Stack=true". Enregistrez ensuite le fichier de script et redémarrez l'IDE CA Workflow.
- **Tomcat** : tenez compte des renseignements suivants :
  - Si vous avez des difficultés avec le démarrage de Tomcat, et que par conséquent, CA Workflow et l'interface Web ne sont pas disponibles, augmentez la mémoire de Tomcat.

    Remarque : Pour de plus amples renseignements sur la résolution de ce problème, consultez l'article TEC418959 de la base de connaissances à l'adresse http://www.ca.com/worldwide.

- Pendant l'installation de CA Workflow, CA SDM et CA EEM utilisent un numéro de port distinct pour Tomcat. Si vous rencontrez des difficultés avec Tomcat lors de l'installation ou de l'utilisation de CA Workflow, arrêtez et redémarrez (page 279) le service.
- Le nom d'hôte de CA Workflow que vous spécifiez dans le gestionnaire d'options *doit* correspondre à la variable NX_LOCAL_HOST dans le fichier NX.env du serveur sur lequel vous avez installé CA Workflow. Le nom d'hôte *doit* également respecter la casse appropriée.
- Si vous avez installé et modifié les valeurs d'installation par défaut pour le port Tomcat (8080) ou l'ID d'utilisateur/mot de passe de l'utilisateur à forts privilèges par défaut (ServiceDesk/ServiceDesk), vous devez apporter les modifications suivantes aux définitions/acteurs par défaut de CA Workflow pour que ceux-ci fonctionnent correctement.
- Connectez-vous à l'environnement de conception (IDE) de flux de travaux.

  Suivez les étapes ci-dessous pour modifier l'Acteur de service Web CA Service Desk par défaut.

  a. Cliquez sur l'onglet Acteurs.

  b. Développez l'arborescence des services Web.

  c. Avec le bouton droit de la souris, cliquez sur l'acteur Unicenter_Service_Desk_Web_Service et sélectionnez Propriétés.

  d. Sélectionnez et copiez le contenu de l'entrée d'URL WSDL.

  e. Modifiez le nom de l'acteur, puis cliquez sur OK.

  f. Cliquez avec le bouton droit de la souris sur l'arborescence des services Web et sélectionnez Add Actor.

  g. Dans le champ Nom, entrez **Unicenter_Service_Desk_Web_Servic**e.

  h. Dans l'entrée d'URL de WSDL, collez le contenu que vous avez copié antérieurement.

  i. Dans l'URL, modifiez le numéro de port afin qu'il corresponde au numéro de port sélectionné lors de la configuration de Tomcat.

  j. Cliquez sur OK.
- Après l'installation de CA Workflow sur le serveur CA SDM, utilisez la procédure suivante afin que l'intégration entre CA SDM et CA Workflow fonctionne correctement :

  - Connectez-vous à CA Workflow IDE pour modifier l'Acteur de service Web CA SDM par défaut.
  - Sélectionnez l'onglet Acteurs, développez l'arborescence JavaScript, et cliquez sur USD Initializer.
  - Double-cliquez sur l'option d'obtention d'attributs globaux.

- Sous la section de script, entrez le nom et le mot de passe de l'utilisateur à forts privilèges CA SDM dans les champs suivants :

  USD_Username = ""

  USD_Password = ""

- Modifiez ces valeurs dans le fichier $NX_ROOT/data/workflow/actors/r12_Service_Desk_Actors_en_US.xml.

Renseignements supplémentaires :

Installation de CA Workflow (page 228)

Utilitaire de migration de flux de travaux

L'outil de migration de données de flux de travaux permet de déplacer des données d'une base de données de CA Workflow vers un autre. Cet utilitaire peut déplacer des données de l'une des bases de données prises en charge vers une autre, et peut déplacer des données selon le schéma de CA Workflow le plus récent.

L'outil de migration de données de flux de travaux est fourni en tant que IU et en tant que bean.

- **IU** : migration.jar
- **Bean** : datamover.jar

Remarque : Pour exécuter ces commandes Java, deux fichiers JAR (datamover.jar et migration.jar) doivent être décompressés manuellement et extraits dans le chemin d'accès Java. Le fichier Migration.zip peut être recherché sur les médias d'installation dans le répertoire \winsrvr.cd1\CA_tps.nt\CAFLOW\Resources.

Exécutez l'utilitaire de migration à partir de la ligne de commande

L'outil de migration est fourni comme bean dans datamover.jar. Vous pouvez exécuter l'outil de migration à partir de la ligne de commande.

Exécutez l'utilitaire de migration.

```
java -cp <driver jar file(s)> com.ca.workflow.util.DataMover <source db driver name> <source db url> <source db username> <source db password> <target db driver name> <target db url> <target db username> <target db password> <number of entries in one transaction> [product keys (comma separated)]--fetchsize=15 [options]
```

Exemple :

```
java -cp iijdbc.jar;datamover.jar com.ca.workflow.util.DataMover
ca.ingres.jdbc.IngresDriver
jdbc:ingres://155.35.26.105:EI7/mdb;cursor=readonly;auto=multi;group=workflow_adm
in_group root iloveca ca.ingres.jdbc.IngresDriver
jdbc:ingres://tadra01-w2k3-v:EI7/mdb;cursor=readonly;auto=multi;group=workflow_ad
min_group tadra01 ca#33333 50 wekProductKey1 --clean-target --fetchsize=15
```

Fichier(s) jar du pilote

Identifie le(s) fichier(s) source et cible du pilote. Séparez plusieurs fichiers de pilote à l'aide de points-virgules (;).

nom du pilote de la base de données source

Identifie le pilote de la base de données source.

URL de la base de données source

Identifie l'URL de la base de données source.

nom de l'utilisateur de la base de données source

Identifie l'utilisateur de la base de données source.

mot de passe de la base de données source

Identifie le mot de passe de la base de données source.

nom du pilote de la base de données cible

Identifie le pilote de la base de données cible.

URL de la base de données cible

Identifie l'URL de la base de données cible.

nom de l'utilisateur de la base de données cible

Identifie l'utilisateur de la base de données cible.

mot de passe de la base de données cible

Identifie le mot de passe de la base de données cible.

nombre d'entrées dans une transaction

Spécifie le nombre d'entrées à déplacer dans une transaction. Si ce nombre est trop grand, il existe une possibilité d'envahir le journal de transactions d'Ingres. Le port par défaut recommandé est 50.

nettoyer la cible

Supprime toutes les données associées aux clé(s) de produit de la base de données cible avant le début du transfert de données. Si aucune clé de produit n'est spécifiée, toutes les données sont supprimées de la base de données cible avant le début du transfert de données. Cette option peut être utilisée pour nettoyer une base de données cible si une migration antérieure a échoué en cours d'exécution.

fetchsize

Si l'option de ligne de commande -fetchsize est présente, elle spécifie le nombre de lignes devant être extraites en une fois dans une liste déroulante de résultats. Si elle n'est pas spécifiée, l'utilitaire utilise la ligne de commande fetchsize par défaut de la base de données source. Ingres ne possède pas de valeur par défaut pour le nombre de lignes à extraire à la fois dans une liste déroulante de résultats ; dans ce cas, la valeur par défaut de 10 lignes sera utilisée si elle n'est pas spécifiée comme option de ligne de commande.

clés de produit

Spécifie les clés de produit pour lesquelles les données doivent être migrées. Il s'agit d'un paramètre facultatif. S'il est spécifié, il peut s'agir d'une clé de produit unique ou d'une liste de plusieurs clés de produits séparées par des virgules. Si le paramètre de clés de produit est présent, l'utilitaire de migration migre uniquement les données à partir de la base de données source qui est contrainte par les clés de produit spécifiées. Si ce paramètre est omis, toutes les données de flux de travaux sont migrées sans tenir en compte de la clé de produit.

Fichier journal

Un fichier journal est créé quand vous transférez des données à partir d'une ligne de commande.

<fichier> ...

Tous les fichiers de pilotes doivent être placés dans le répertoire de l'outil de migration ou vous devez spécifier l'emplacement du fichier JAR du pilote de la base de données.

Exécutez l'utilitaire de migration à partir de l'IU

Pour exécuter la migration à partir de l'IU

1. Dans la ligne de commande, entrez la commande suivante :

   ```
   java -cp datamover.jar;migration.jar -Dwflog="c:\wf.log"  -Dtxlimit="0"
   com.ca.workflow.util.WFMigration
   ```

   La boîte de dialogue Outil de migration des données de flux de travaux apparaît.

2. Pour les sections Source Database et Target Database, sélectionnez le type de base de données dans le menu déroulant Database Type.

   Les noms et les URL des pilotes sont mis à jour automatiquement. Vous pouvez modifier ces valeurs par défaut, si nécessaire.

   - Pour Ingres, utilisez -iijdbc.jar
   - Pour Oracle 10g, utilisez ojdbc14.jar
   - Pour Oracle 11g, utilisez ojdbc5.jar
   - Pour MS SQL 2000, utilisez msutil.jar, msbase.jar, mssqlserver.jar

- Pour MS SQL 2005, utilisez sqljdbc.jar
- Pour Sybase Adaptive Server Enterprise 12.5.4, utilisez jconn3.jar
- Pour Sybase Adaptive Server Enterprise 15.0, utilisez jconn3.jar

Important : Pour connaître la liste des bases de données prises en charge pour CA SDM, reportez-vous aux *Notes de parution*.

3. Renseignez les champs appropriés.
4. Cliquez sur Démarrer.

   La migration des données commence. Pendant la migration, l'état est mis à jour en bas de la boîte de dialogue.

Planification d'intégration de CA Process Automation

CA Process Automation est un produit de CA autonome comportant des fonctionnalités pour automatiser et effectuer le suivi des tâches d'administration de matériel et de logiciel dans des environnements informatiques d'entreprise. CA Process Automation automatise les tâches et gère les interactions d'utilisateur, comme les approbations et les notifications pour la conformité et la précision dans des environnements de production.

Lors de la planification de l'intégration de CA Process Automation, prenez les éléments suivants en considération :

- Prévoyez du temps supplémentaire pour installer et configurer le produit CA Process Automation.
- Déterminez si CA Process Automation et CA SDM peuvent coexister sur un même serveur lorsque l'architecture du serveur prend en charge ces deux produits. Si les composants de CA Process Automation ou de CA SDM ne peuvent pas coexister sur le même serveur, vous devez envisager d'installer ces produits sur des serveurs séparés.
- Prévoyez suffisamment de temps pour vérifier que les deux produits sont installés et qu'ils fonctionnent de façon indépendante.
- Lorsque CA SDM est intégré à CA Process Automation qui utilise CA EEM 8.4, vérifiez que vous appliquez le correctif du SDK CA EEM 8.4 sur CA SDM. Les détails relatifs à ce correctif sont disponibles auprès du service de soutien de CA.

  Remarque : Pour de plus amples renseignements sur les exigences des produits CA SDM et CA Process Automation, reportez-vous aux *Notes de parution de CA SDM*. Pour de plus amples renseignements sur les plates-formes prises en charge par CA Process Automation, sur les étapes requises et sur les options d'installations, reportez-vous à la documentation sur l'installation et la configuration de CA Process Automation.

Remarques relatives à la sécurité

Outre la configuration minimale indiquée dans les notes de parution, prenez les recommandations suivantes en compte lors de l'installation de CA Process Automation :

- Configurez CA Process Automation de façon à ce qu'il utilise CA EEM comme serveur d'authentification. CA EEM empêche que des noms d'utilisateurs et des mots de passe en texte brut ne soient transmis à des fins d'authentification.
- Si vous utilisez l'hébergement multiclient pour CA Process Automation, l'installation de CA EEM est requise.

  Remarque : Pour de plus amples renseignements sur la mise en oeuvre de l'hébergement multiclient avec CA Process Automation, reportez-vous à la documentation relative à l'installation et à la configuration de CA Process Automation.
- Si vous utilisez l'hébergement multiclient pour CA SDM, l'installation de CA EEM est requise.

  Remarque : Si vous n'utilisez pas d'hébergement multiclient, la configuration de CA EEM pour CA SDM est facultative.
- Configurez CA Process Automation pour communiquer en utilisant les communications sécurisées sur HTTPS. Les URL HTTPS utilisent SSL/TLS pour supprimer les échanges de texte brut, protégeant ainsi les données propriétaires, ainsi que d'autres données sensibles, contre une divulgation accidentelle ou malveillante.

  Remarque : Pour de plus amples renseignements sur la façon de configurer CA Process Automation pour utiliser HTTPS, consultez la documentation de l'installation et de la configuration de CA Process Automation.

Configuration des communications SSL avec CA Process Automation

Il se peut que, pour des raisons de sécurité, les programmeurs de CA Process Automation aient choisi d'installer ou de reconfigurer CA Process Automation pour qu'il exige des communications SSL. Si CA Process Automation est configuré pour requérir des communications SSL, les applications intégrées telles que CA SDM requièrent un certificat de l'espace de stockage de clés de CA Process Automation pour les communications.

Pour configurer des communications SSL avec CA Process Automation, procédez de la manière suivante :

1. Configurez les options de CA SDM pour qu'elles utilisent l'adresse HTTPS CA Process Automation.

2. Exportez le certificat de l'espace de stockage de clés de CA Process Automation vers un fichier et copiez ce fichier dans CA SDM.
3. Chargez le fichier de certificat dans CA SDM à l'aide de l'utilitaire pdm_keystore_mgr de CA SDM.
4. Si cela s'applique à votre architecture CA SDM, mettez à jour les fichiers de contrôle de version afin de livrer l'espace de stockage des clés de CA SDM à tous les serveurs secondaires.
5. Redémarrez CA SDM.

Activation des communications lorsque CA Process Automation est compatible avec SSL

Lorsque CA Process Automation communique avec SSL, vous devez configurer les serveurs CA SDM pour qu'ils communiquent avec CA Process Automation.

Pour activer des communications quand CA Process Automation est compatible SSL, procédez de la manière suivante :

1. Assurez-vous que vous pouvez utiliser CA Process Automation dans un navigateur sans lancer CA SDM. Enregistrez l'URL de CA Process Automation pour vous y référer lorsque vous configurez les options de Flux de travaux de CA Process Automation dans le gestionnaire d'options.
2. Connectez-vous à CA SDM et installez ou modifiez les options de Flux de travaux de CA Process Automation dans le gestionnaire d'options. Pour chacune des options suivantes, utilisez la syntaxe *https://server:8443* au lieu de http://server:8080 pour atteindre l'application CA Process Automation compatible SSL. Cependant, si l'installation de CA Process Automation utilise un autre port que le port SSL 8443, spécifiez le numéro de port approprié.
   - caextwf_endpoint
   - caextwf_processdisplay_url
   - caextwf_worklist_url

   Remarque : Si les valeurs ne correspondent pas aux valeurs d'installation de CA Process Automation réelles, CA SDM ne peut pas communiquer avec CA Process Automation et une erreur d'exécution se produit. Vérifiez que les valeurs correspondent aux valeurs réelles d'installation de CA Process Automation car il se peut que le programme d'installation de CA Process Automation ait sélectionné un port différent du port 8443.

3. Sur le serveur CA Process Automation, localisez les entrées KEYSTOREID et itpam.web.keystorealias dans le fichier suivant :

   ```
   C:\Progra~1\ITPAM\server\c2o\.config\0asisConfig.properties
   ```

4. Copiez la valeur KEYSTOREID. Soyez prêt à coller la valeur KEYSTOREID pour l'utiliser en tant que mot de passe après avoir émis la commande keytool.

5. Sur le serveur CA Process Automation, émettez la commande keytool suivante sur la ligne de commande :

   ```
   C:\Progra~1\ca\sc\jre\1.6.0_00\bin\keytool.exe -keystore
   C:\Progra~1\ITPAM\server\c2o\.config\c2okeystore -export -alias
   <keystorealias> -file itpam.cer
   ```

   L'utilitaire keytool vous invite à fournir un mot de passe.

6. Collez ou tapez la valeur KEYSTOREID comme mot de passe.

   L'utilitaire keytool utilise le dernier paramètre (-file itpam.cer) pour créer un fichier nommé *itpam.cer*. Le fichier *itapm.cer* contient les données de certificat nécessaires pour les communications avec CA SDM.

7. Déplacez le fichier *itpam.cer* vers l'un des emplacements suivants sur le serveur CA SDM :

   - (Windows) %NX_ROOT%\bin
   - (UNIX) $NX_ROOT/bin

8. Importez les données de certificat de CA Process Automation dans CA SDM en entrant la commande suivante :

   ```
   (Windows) pdm_perl %NX_ROOT%\bin\pdm_keystore_mgr.pl -import
   %NX_ROOT%\bin\itpam.cer
   (UNIX) pdm_perl $NX_ROOT/bin/pdm_keystore_mgr.pl -import $NX_ROOT/bin itpam.cer
   ```

   Le script *pdm_keystore_mgr.pl* génère le fichier keystore aux emplacements suivants :

   - (Windows) %NX_ROOT%\pdmconf\nx.keystore
   - (UNIX) $NX_ROOT/pdmconf/nx.keystore

9. *nx.keystore* doit être distribué aux serveurs CA SDM suivants, en fonction de la configuration de CA SDM :

   - Conventionnelle : serveur secondaire
   - Disponibilité avancée : serveur d'applications et de secours

   Ouvrez le fichier *server_custom.ver* depuis l'un des emplacements suivants :

   - (Windows) %NX_ROOT%\site\server_secondary.ver
   - (UNIX) $NX_ROOT/site/server_secondary.ver

10. Modifiez *server_secondary.ver* pour le contrôle de version en ajoutant les données suivantes :

```
[SSL_Keystore]
filename = "nx.keystore"
directory = "$NX_ROOT/pdmconf"
component_type = "file"
O_mode = "RW"
g_mode = "RW"
w_mode = "RW"
file_ctl
```

    Remarque : Pour de plus amples renseignements sur la gestion du contrôle de version , reportez-vous au *Manuel d'administration*.

11. Redémarrez CA SDM.

    Le serveur CA SDM peut communiquer avec l'application CA Process Automation compatible SSL.

Remarque : Pour de plus amples renseignements sur la configuration des options de flux de travaux de CA Process Automation, reportez-vous à l'*Aide en ligne*.

Planification de l'installation de CA Business Intelligence

Pour vous aider à planifier l'installation et la configuration de CA Business Intelligence, utilisez les informations suivantes pour rechercher et rassembler des informations.

- **Recherche** : effectuez les opérations suivantes :
  - Lisez les notes de parution pour comprendre les exigences pour CA Business Intelligence.
  - Lisez votre documentation de CA Business Intelligence, y compris les notes de parution et le fichier Readme facultatif (si disponible).

  Remarque : Pour une liste détaillée des environnements pris en charge et de la configuration matérielle requise, reportez-vous aux différents documents des plates-formes prises en charge sur le DVD CA Business Intelligence. Ces documents incluent les exigences en termes de correctifs et de version spécifique pour les serveurs d'applications Web, les navigateurs Web et les systèmes d'exploitation.

- **Répertoire de base d'installation** : déterminez le répertoire de base dans lequel vous voulez installer CA Business Intelligence. Les emplacements par défaut sont les suivants :
  - Pour des ordinateurs 32bit de Windows : C:\Program Files\CA\SC\CommonReporting3
  - Pour des ordinateurs x64 : C:\Program Files X(86)\CA\SC\CommonReporting3

  Si ce répertoire n'existe pas, créez-le avant de démarrer l'installation.
- **Logiciels antivirus** : désactivez temporairement tout logiciel d'analyse antivirus sur l'ordinateur sur lequel vous installez CA Business Intelligence.
- **Serveurs d'applications pris en charge** : l'intégration de CA SDM avec CA Business Intelligence prend uniquement en charge Apache Tomcat en tant que serveur d'applications CA Business Intelligence.
- **Navigateurs Web pris en charge :** CA Business Intelligence 3.2 SP5 prend en charge les navigateurs Web suivants :

Système d'exploitation du navigateur	Navigateur	Ordinateur virtuel Java
Apple Mac OS X	Safari 5	Apple 1.6.0_xx
Microsoft Windows	Firefox 3.6	Sun 1.5.0._xx Sun 1.6.0_xx
	Firefox 8 **Remarque :** Les nouvelles versions de Firefox seront prises en charge pour la phase de test minimal d'environ deux semaines après leur publication par Mozilla.	Sun 1.6.0_xx
	Internet Explorer 6.0 SP3	Sun 1.5.0_xx Sun 1.6.0_02+
	Internet Explorer 7.0	Sun 1.5.0_xx Sun 1.6.0_02+
	Internet Explorer 8.0 **Remarque :** Seul le mode compatible est pris en charge.	Sun 1.6.0_xx
	Internet Explorer 9.0 **Remarque :** Seul le mode compatible est pris en charge.	Sun 1.6.0_xx

Important : L'installation de CA Business Intelligence est limitée aux plates-formes Windows uniquement pour CA SDM r12.9. Cependant, vous pouvez intégrer CA Business Intelligence à CA SDM sur tous les systèmes d'exploitation pris en charge.

Remarques relatives au signalement

Avant d'installer CA Business Intelligence, tenez compte des informations suivantes pour assurer une mise en oeuvre réussie :

- Une installation de CA Business Intelligence r3.2 (BusinessObjects Enterprise version 3.1) est requise pour afficher les rapports de CA SDM r12.9 inclus dans cette version.
- CA Business Intelligence r2.1 (BusinessObjects Enterprise version 2) n'est pas pris en charge.
- Vous pouvez installer CA Business Intelligence r3.0 pendant le processus de mise à niveau de r12.1 à r12.5.
- L'installation diffère en fonction du type d'installation sélectionné.
- Les informations d'identification d'administrateur BusinessObjects sont nécessaires pour pouvoir lancer le programme d'installation, que ce soit pour l'installation standard ou personnalisée.
- CMS (Configuration Management Server) doit être installé sur le port 6400 (par défaut) ; dans le cas contraire, la configuration de CA Business Intelligence échoue pendant l'installation.
- Les utilisateurs de CA SDM doivent être ajoutés à la liste de l'administrateur dans CMS avant d'utiliser les rapports.
- Vous devez effectuer quelques étapes de configuration supplémentaires si vous voulez installer Apache Tomcat 5.5.20 en vue d'une utilisation en tant que serveur d'applications BusinessObjects.
- Les utilisateurs de SAP Business Objects ayant une installation existante de Business Objects peuvent installer et configurer CA Business Intelligence (recommandé) ou utiliser leur installation Business Objects existante.
- Si vous prévoyez d'accéder à InfoView avec Firefox, vous devez utiliser la version de Firefox prise en charge par CA Business Intelligence 3.2.
- Il se peut que vous deviez modifier la version du JRE fourni avec Business Objects pour une version mieux adaptée à votre environnement spécifique.
- Crystal Reports Explorer et Desktop Intelligence ne sont *pas* pris en charge, même s'ils peuvent être appelés après l'installation de CA Business Intelligence.

Nouvelle installation par rapport à Installation personnalisée (Windows)

Plusieurs différences existent entre une nouvelle installation et une installation personnalisée. Le flux de l'installation diffère selon le type d'installation que vous sélectionnez.

nouveau

Installe tous les composants sur un ordinateur. Sélectionnez ce type d'installation pour configurer rapidement un déploiement complet, avec tous les composants serveur et clients sur un seul ordinateur. Une nouvelle installation fournit :

- MySQL comme base de données pour stocker les informations du CMS.
- Apache Tomcat comme serveur d'applications

Remarque : BusinessObjects Enterprise requiert une base de données pour stocker des informations sur les utilisateurs et les groupes, les niveaux de sécurité, le contenu BusinessObjects Enterprise et les serveurs. La base de données principale, que le serveur de gestion centralisée préserve, est connue sous le nom de base de données CMS. Pendant l'installation de CA Business Intelligence, spécifiez la base de données CMS à utiliser, puis entrez les paramètres nécessaires à l'authentification. Pour plus d'informations sur la configuration système requise et la préparation de la base de données CMS, reportez-vous au *Manuel de mise en oeuvre de CA Business Intelligence*.

Personnalisée

Installe les composants que vous sélectionnez sur l'ordinateur. Sélectionnez ce type d'installation pour spécifier quels composants installer lorsque vous effectuez un déploiement réparti ou que vous ajoutez des serveurs à un déploiement existant.

Important : Effectuez une installation personnalisée si vous installez le CMS BusinessObjects sur une base de données Microsoft SQL ou Oracle.

Une installation personnalisée dispose d'options permettant d'effectuer les actions suivantes.

Installez MySQL ou utilisez un CMS pré-existant, dont :

- Oracle
- Microsoft SQL
- Apache Tomcat : vous pouvez contrôler l'installation de l'instance Apache Tomcat.

Informations d'identification d'administrateur BusinessObjects

Le mot de passe d'administrateur BusinessObjects est nécessaire pour pouvoir lancer le programme d'installation, que ce soit pour l'installation standard ou personnalisée.

Ce mot de passe doit inclure des minuscules et des majuscules, contenir au moins six caractères et ne peut pas contenir le mot administrateur sous quelque forme que ce soit. Il doit également contenir au moins deux des types de caractères suivants.

- Majuscules
- Minuscules
- Numérique
- Ponctuation

Serveur d'applications de BusinessObjects Enterprise XI

BusinessObjects Enterprise nécessite un serveur d'applications pour traiter les scripts côté serveur formant les applications Web.

Pendant l'installation de CA Business Intelligence, vous spécifiez le serveur d'applications à utiliser et vous entrez les paramètres de configuration requis. CA Business Intelligence propose d'installer Apache Tomcat 5.5.20. Vous pouvez également utiliser votre serveur d'applications existant.

Si vous choisissez d'installer Apache Tomcat 5.5.20 comme serveur d'applications BusinessObjects, vous devez procéder comme suit :

- Installez Java 2 Standard Edition JDK 1.5.
- Définissez la variable d'environnement $JAVA_HOME sur le répertoire de base de JDK 1.5.
- Installez Apache Tomcat 5.5.20 et définissez le chemin d'accès de l'ordinateur virtuel Java vers le répertoire dans lequel Java 2 Standard Edition JRE 1.6 est installé sur votre système.
- Effectuer une installation personnalisée de CA Business Intelligence.
- Dans la fenêtre de configuration du serveur Web, sélectionnez "Non" lorsque vous êtes invité à installer une nouvelle copie de Tomcat pour BusinessObjects XI.
- Sélectionnez Tomcat dans la liste des serveurs d'applications.
- Entrez l'emplacement du serveur Web Apache Tomcat 5.5.20 dans le champ Répertoire d'installation et terminez l'installation.
- Après avoir terminé l'installation de CA Business Intelligence, exécutez la configuration de CA Business Intelligence.

Remarque : Si vous avez déjà installé CA Business Intelligence avec JDK 1.5 (à l'aide d'un serveur d'applications externe autre que le serveur par défaut) et que vous souhaitez utiliser JRE 1.6 sur un environnement client ayant accès à l'outil InfoView Web Intelligence, n'installez pas JRE 1.4.2 lorsque vous y êtes invité. Installez plutôt JRE 1.6 sur l'environnement client. Le cas échéant, redémarrez votre navigateur après avoir installé JRE 1.6. Vous pouvez télécharger JRE 1.6 à partir du site Web d'Oracle.

Installation existante de BusinessObjects (SAP)

Si vous êtes un utilisateur BusinessObjects de SAP et que vous avez une installation existante de BusinessObjects qui n'a pas été installée par CA Business Intelligence, nous vous recommandons d'installer et de configurer CA Business Intelligence, pour assurer une compatibilité et une prise en charge optimales. Si vous préférez utiliser votre installation BusinessObjects existante, vous pouvez ignorer les étapes d'installation de CA Business Intelligence et passer à la section Configuration de CA Business Intelligence.

Remarque: Vous devez utiliser la version 3 de BusinessObjects Enterprise et déployer Tomcat comme serveur d'applications. Vous devez aussi disposer d'une licence pour Web Intelligence. Quant à Crystal Reports, vous devez avoir une licence d'exécution ou supérieure.

Accès à InfoView avec Firefox

Si vous souhaitez accéder à BusinessObjects InfoView avec Firefox, vous devez utiliser Firefox 2 avec machine virtuelle Java (Java Runtime) 1.5.0_xx et 1.6.0_02+.

Remarque : Pour plus d'informations sur les plates-formes et niveaux de version pris en charge, reportez-vous au *Manuel de BusinessObjects Enterprise XI pour Windows*.

Meilleures pratiques de signalement

Appliquez les bonnes pratiques suivantes lorsque vous installez, conservez et utilisez CA Business Intelligence :

- Installez et conservez un univers pour chaque produit CA. Le cas échéant, vous pouvez créer des univers reliés.
- Avant d'appliquer des services packs, des correctifs et d'autres mises à jour à votre univers personnalisé, sauvegardez toutes vos personnalisations.
- Ne modifiez pas l'univers par défaut. A la place, copiez-le et modifiez la copie. Sans cela, vos personnalisations risquent d'être effacées lorsque vous appliquerez des services packs, des correctifs ou d'autres mises à niveau.
- Créez vos propres dossiers.
- Si les rapports cessent de s'exécuter, assurez-vous que le CMS (Central Management Server) s'exécute.
- N'écrasez pas les rapports prédéfinis.
- Utilisez toujours un rapport prédéfini comme base pour la création d'un rapport personnalisé. Ce mode d'opération contribue à appliquer un formatage homogène à tous les rapports.

Remarque: Pour plus d'informations sur l'accomplissement de ces tâches, reportez-vous à la documentation de BusinessObjects Enterprise.

Stratégies de mise en oeuvre

Lorsque vous planifiez votre stratégie de mise en oeuvre de CA Service Desk, tenez compte des renseignements suivants, en plus de la disponibilité, de la bande passante utilisable et de la capacité de réaction du réseau.

- **Centralisée** : installe et configure tous les composants du produit sur un serveur principal. Il s'agit de l'installation par défaut. Vous pouvez exécuter plusieurs gestionnaires d'objets et moteurs Web pour l'équilibrage de la charge et le basculement, mais cette mise en oeuvre peut se révéler insuffisante pour vos activités.

- **Répartie** : installe et configure les composants du produit sur des serveurs qui sont plus proches des clients recevant le service. Par exemple, le bureau d'une entreprise qui dispose de plusieurs sous-réseaux peut compter de nombreux analystes qui utilisent le client Web. Placer un serveur secondaire dans ce bureau permet de réduire le trafic réseau et les temps de réponse. Le trafic réseau entre le bureau et l'emplacement du serveur principal est également réduit parce que le serveur secondaire effectue une mise en cache. Ce type de mise en oeuvre prend en charge la mise en oeuvre de plusieurs gestionnaires d'objets et moteurs Web pour l'équilibrage de la charge et le basculement.
- **Globale** : se compose d'au moins deux mises en oeuvre centralisées ou réparties, appelées régions. Le serveur principal d'une région copie les données minimales depuis et vers une région maîtresse. Cela permet à une région d'avoir toutes les données nécessaires sur toutes les autres régions. Cela permet à un analyste d'être au courant des billets de toutes les régions, mais de se connecter uniquement à une région lorsque c'est nécessaire. Ce type de mise en oeuvre est utile quand la bande passante du réseau est trop limitée pour une mise en oeuvre répartie. Par exemple, vous pouvez disposer de bureaux dans différents pays reliés par une liaison lente.

Remarque : Pour de plus amples renseignements, reportez-vous à la section Architecture CA Service Desk pour la disponibilité avancée (page 89).

Activer l'authentification Windows dans Firefox

L'authentification du gestionnaire de réseau local Windows NT (NTLM) permet aux informations d'identification de connexion d'un utilisateur Windows, qui est connecté à un domaine Windows, d'être automatiquement transférées vers un serveur Web IIS dans le même domaine. Par défaut, l'authentification Windows n'est pas activée dans Firefox. Pour préparer votre mise en oeuvre, vous devez activer l'authentification Windows dans Firefox.

Pour activer l'authentification Windows dans Firefox

1. Démarrez Firefox.
2. Accédez à l'URL suivante :

   about:config
3. Confirmez que vous voulez modifier les paramètres avancés.

   La liste des noms de préférences apparaît.
4. Recherchez le nom de préférence *network.automatic-ntlm-auth.trusted-uris* et cliquez deux fois dessus :

   La boîte de dialogue vous invitant à entrer une valeur de chaîne apparaît.

5. Spécifiez la liste de sites fiables en entrant l'URL complète (par exemple, http://web.exemple.com) ou le nom de serveur (par exemple, web.exemple.com)

   Remarque : N'entrez pas de barre oblique finale. Si vous voulez spécifier plusieurs serveurs, séparez-les par une virgule. Vous pouvez indiquer tous les serveurs d'un domaine particulier, mais les caractères génériques standard ne fonctionnent pas. Par exemple, vous devez spécifier *.example.com* plutôt que **.example.com*.

6. Cliquez sur OK.

7. Redémarrez Firefox.

Chapitre 4: Installation

Ce chapitre traite des sujets suivants :

Mise en oeuvre du logiciel (page 137)
Configuration des serveurs CA SDM (page 138)
Procédure de conversion de la configuration conventionnelle en configuration de disponibilité avancée (page 146)
Procédure de conversion de la configuration de disponibilité avancée en conventionnelle (page 151)
Installation de la CA MDB (page 155)
Installation de CA SDM (page 163)
Installation de l'Outil de conception Web (page 177)
Installation et configuration de l'intégration de CA SDM et CA NSM (page 178)
Installation de CA EEM (page 224)
Installation de CA Workflow (page 228)
Installation de CA Business Intelligence pour CA SDM (page 231)
Vérification de l'installation (page 235)
Fichier journal d'installation (page 236)

Mise en oeuvre du logiciel

Vous mettez en oeuvre CA SDM en fonction d'un certain nombre de facteurs, comme le fait que vous effectuiez ou non une mise à niveau à partir d'une version antérieure, le fait que vous installiez le produit pour la première fois, votre système d'exploitation, votre base de données, les produits que vous voulez intégrer, etc. En général, suivez cette procédure pour exécuter le logiciel :

1. Lisez les remarques concernant la mise en oeuvre qui sont documentées dans les *Notes de parution*.
2. Si vous effectuez une *mise à niveau* à partir d'une version antérieure, suivez les étapes pour mettre à niveau la base de données, la console et CA Workflow.
3. Installez CA MDB.

   Si votre base de données (SQL Server ou Oracle) est installée sur un serveur autre que le serveur principal de CA SDM, installez la CA MDB sur le serveur de base de données distant (c'est-à-dire, l'ordinateur sur lequel SQL Server ou Oracle est installé). Si la CA MDB et le serveur principal sont sur le même ordinateur, CA MDB s'installe automatiquement.
4. Installez CA SDM sur le serveur principal ou sur le serveur secondaire facultatif.

   Vous pouvez personnaliser les formulaires Web et le schéma après l'installation parce que l'Outil de conception Web s'installe automatiquement sur le serveur.

5. (Facultatif) Activez le visualiseur CA CMDB pendant la configuration de CA SDM.
6. (Facultatif) Activez Automatisation du soutien pendant la configuration de CA SDM.

   Important : Si vous voulez migrer des divisions de CA Automatisation du soutien r6.0 SR1 eFix5 vers des clients hébergés, convertissez ces données avant d'activer et de configurer Automatisation du soutien dans CA SDM r12.9.
7. (Facultatif) Activez l'API REST lors de la configuration CA SDM.
8. (Facultatif) Installez CA EEM pour l'authentification.
9. (Facultatif) Installez CA Workflow pour gérer vos processus commerciaux.
10. (Facultatif) Installez CA Business Intelligence pour gérer les rapports avec la technologie BusinessObjects.
11. (Facultatif) Installez l'intégration de CA NSM.

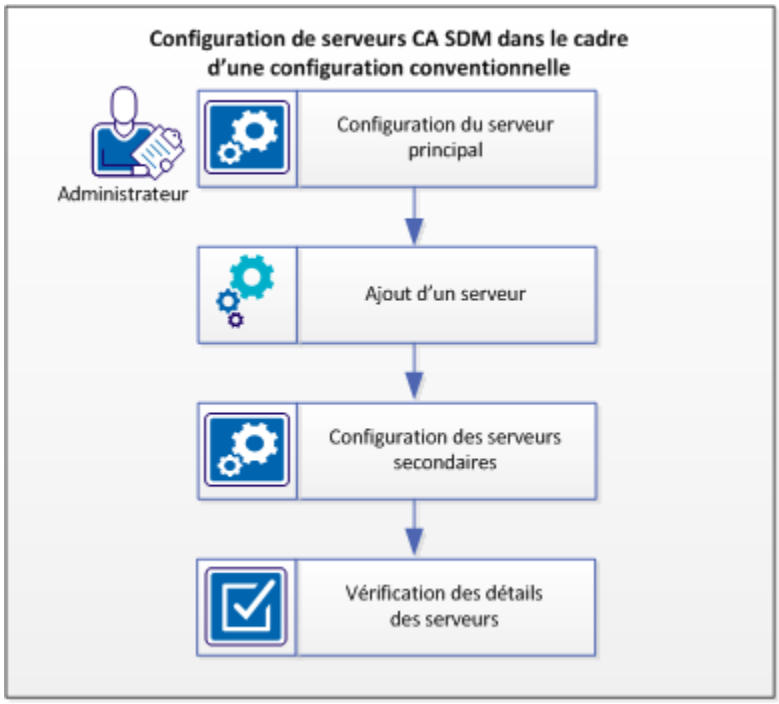
Configuration des serveurs CA SDM

En tant qu'administrateur système, vous pouvez configurer les serveurs CA SDMdans les cas suivants :

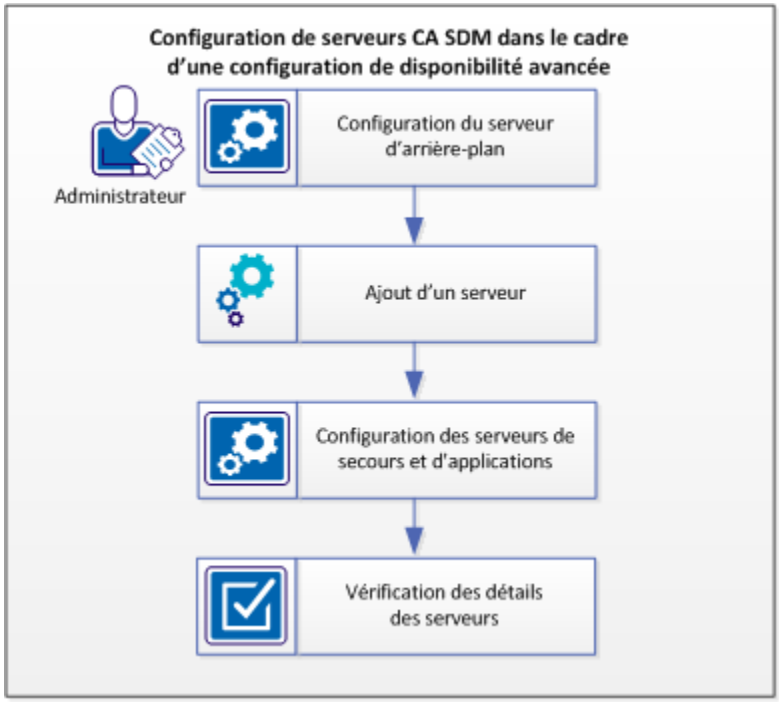
- Vous avez exécuté une nouvelle installation de CA SDM et souhaitez implémenter la configuration de disponibilité avancée ou la configuration conventionnelle.
- Vous avez effectué une mise à niveau vers la dernière version de CA SDM et souhaitez implémenter la configuration de disponibilité avancée ou la configuration conventionnelle.

Remarque : Si vous avez installé CA SDM ou l'avez mis à niveau avec une configuration particulière (conventionnelle, par exemple) et voulez implémenter l'autre configuration (disponibilité avancée, par exemple), reportez-vous aux scénarios de conversion ou au *Manuel de mise en oeuvre*.

Le diagramme suivant montre la procédure de configuration des serveurs CA SDM dans une configuration conventionnelle :


Configuration de serveurs CA SDM dans le cadre d'une configuration conventionnelle
Administrateur
Configuration du serveur principal
Ajout d'un serveur
Configuration des serveurs secondaires
Vérification des détails des serveurs

Le diagramme suivant montre la procédure de configuration des serveurs CA SDM dans une configuration de disponibilité avancée :


Configuration de serveurs CA SDM dans le cadre d'une configuration de disponibilité avancée
Administrateur
Configuration du serveur d'arrière-plan
Ajout d'un serveur
Configuration des serveurs de secours et d'applications
Vérification des détails des serveurs

1. Selon votre configuration de CA SDM :
   - Configurez le serveur principal (page 140).
   - Configuration du serveur d'arrière-plan (page 142)
2. Ajoutez un serveur (page 140), si vous n'avez actuellement pas de serveur.
3. Selon votre configuration de CA SDM :
   - Configurez les serveurs secondaires (page 142).
   - Configurez les serveurs de secours et d'applications. (page 143)
4. Vérifiez les détails du serveur (page 145).

Configuration du serveur principal

Le serveur principal doit être configuré avant que vous ne puissiez configurer de serveurs secondaires.

1. Connectez-vous au serveur que vous voulez configurer comme serveur principal.
2. Utilisez la commande pdm_configure pour démarrer la configuration.

   La fenêtre Sélectionner une configuration de serveur s'ouvre.
3. Sélectionnez Conventionnelle comme type de configuration et suivez les invites pour réaliser la configuration. Pour de plus amples renseignements, reportez-vous à l'*Aide sur la configuration de serveurs*.

   Le serveur principal est désormais configuré.

Ajout d'un serveur

Si vous n'avez aucun serveur, ajoutez des enregistrements de serveur pour tous les serveurs que vous souhaitez installer dans votre déploiement CA SDM.

1. Connectez-vous au serveur suivant, selon votre configuration de CA SDM :
   - Conventionnelle : serveur principal
   - Disponibilité avancée : serveur d'arrière-plan

2. Sélectionnez Système, Serveurs sous l'onglet Administration.

   La page Liste des serveurs s'affiche.

3. Cliquez sur Créer pour ajouter un enregistrement de serveur pour le serveur suivant, selon la configuration CA SDM :

   - Conventionnelle : serveur secondaire
   - Disponibilité avancée : serveur d'applications ou de secours

   La page Créer un serveur s'ouvre.

4. Remplissez les champs de serveur appropriés au serveur.
5. Cliquez sur Enregistrer.

   Les détails du serveur ont été ajoutés.

Champs de création d'un serveur

Les champs suivants s'affichent lorsque vous créez un serveur :

Nom d'hôte

Spécifie le nom d'hôte local du serveur. Le nom d'hôte local est stocké dans la table usp_servers dans la colonne local_host.

Important : Assurez-vous que le nom d'hôte entré respecte la casse dans la table usp_servers.

Fuseau horaire

Spécifie le fuseau horaire où le serveur est situé. Le fuseau horaire est utilisé pour déclencher des événements dans le système si l'option Utiliser le fuseau horaire de l'utilisateur final n'est pas sélectionnée ou si aucun fuseau horaire n'est spécifié pour le type de service.

État de l'enregistrement

Indique l'état du serveur. L'état Activé indique que le serveur est inclus dans le déploiement de CA SDM.

Important : Si vous avez désactivé un serveur, il est recommandé de ne pas démarrer de service CA SDM sur ce serveur. Une telle action peut causer un comportement inattendu.

Type de serveur

Spécifie le type de serveur à configurer. Selon votre configuration CA SDM, vous pouvez sélectionner les types de serveurs suivants :

- Disponibilité avancée : serveur d'applications ou de secours
- Conventionnelle : serveur secondaire

Configuré

Disponible uniquement pour la configuration de disponibilité avancée. Indique l'état du serveur configuré. La valeur par défaut de ce champ est Non. Elle passe à Oui après l'exécution de pdm_configure sur ce serveur. Si vous modifiez l'une des valeurs de champs entrées automatiquement pour un enregistrement de serveur, la valeur du champ Configuré(e) passe à Non.

Configuration des serveurs secondaires

Vous configurerez chacun des serveurs secondaires après avoir configuré le serveur principal. Cette configuration est requise pour établir la communication avec le serveur principal.

1. Connectez-vous au serveur que vous voulez configurer comme serveur secondaire.
2. Utilisez la commande pdm_configure pour démarrer la configuration.

   La fenêtre Sélectionner une configuration de serveur s'ouvre.
3. Sélectionnez Conventionnelle comme type de configuration et suivez les invites pour réaliser la configuration. Pour de plus amples renseignements, reportez-vous à l'*Aide sur la configuration de serveurs*.

   Le serveur secondaire est désormais configuré.
4. Répétez les étapes 1 à 3 sur chaque serveur à configurer comme serveur secondaire.

Configuration du serveur d'arrière-plan

Configurez le serveur d'arrière-plan avant de configurer les serveurs d'applications ou de secours.

1. Connectez-vous au serveur que vous voulez configurer comme serveur d'arrière-plan.

2. Utilisez la commande pdm_configure pour démarrer la configuration.

   La fenêtre Sélectionner une configuration de serveur s'ouvre.

3. Sélectionnez Disponibilité avancée comme type de configuration et suivez les invites pour réaliser la configuration. Pour de plus amples renseignements, reportez-vous à l'*Aide sur la configuration de serveurs*.

   Le serveur d'arrière-plan est désormais configuré.

Configuration du serveur de secours ou d'applications

Une fois le serveur d'arrière-plan configuré, configurez chaque serveur de secours et d'applications. Cette configuration est requise pour établir la communication avec le serveur d'arrière-plan.

Important : (Recommandé) Veillez à ce que la configuration du serveur d'arrière-plan et de tous les autres serveurs de secours soit identique. Ce processus permet au serveur de secours de fonctionner comme le serveur d'arrière-plan lors d'un basculement.

1. Connectez-vous au serveur que vous voulez configurer comme serveur de secours ou d'applications.
2. Utilisez la commande pdm_configure pour démarrer la configuration.

   La fenêtre Sélectionner une configuration de serveur s'ouvre.

3. Sélectionnez Disponibilité avancée comme type de configuration et suivez les invites pour réaliser la configuration. Pour de plus amples renseignements, reportez-vous à l'*Aide sur la configuration de serveurs*.

4. Répétez les étapes 1 à 3 pour chaque serveur à configurer comme serveur de secours et d'applications.

   Vous avez configuré les serveurs de secours et d'applications.

5. Configurez l'équilibreur de charge (page 144) si vous disposez d'un ou de plusieurs serveurs d'applications et que vous souhaitez l'utiliser pour suivre les demandes à destination et en provenance de différents serveurs d'applications.

   Remarque : Pour utiliser une URL d'équilibreur de charge ou d'un serveur d'applications pour les liens qui se trouvent dans les notifications CA SDM, procédez comme suit :

   a. Connectez-vous au serveur d'arrière-plan.

   b. Sous l'onglet Administration, sélectionnez Gestionnaire d'options, Notifications.

   c. Remplacez la valeur de l'option web_cgi_url afin qu'elle pointe vers les éléments ci-dessous.

      - L'équilibreur de charge, si vous disposez de plusieurs serveurs d'applications.
      - Le serveur d'applications, si vous en avez un seul.

Configuration de l'équilibreur de charge

Si vous utilisez un ou plusieurs serveurs d'applications, configurez l'équilibrer de changer afin qu'il surveille les serveurs d'applications.

1. Connectez-vous à un serveur d'applications.
2. Copier le fichier HealthServlet.war se trouvant dans le dossier $NX_ROOT/samples/HealthServlet dans le dossier $NX_ROOT/bopcfg/www/CATALINA_BASE/webapps.
3. Redémarrez les services CA SDM ou redémarrez CA SDM Tomcat.
4. Répétez les étapes 1 à 3 pour tous les serveurs d'applications.
5. Configurez l'équilibreur de charge pour qu'il surveille l'URL du healthservlet suivant, sur chacun des serveurs d'applications :

   ```
   http://<Machine_name>:<Port_number>/HealthServlet/GetHealth
   ```

   - Si l'URL du healthservet reçoit une réponse de suspension d'un serveur d'applications, l'équilibreur de charge doit alors rediriger toutes les demandes de ce serveur vers l'autre serveur d'applications. Par exemple, la réponse suivante est reçue lorsque le serveur d'applications est suspendu pendant 58677 secondes.

     ```
     Durée de suspension restante : 58677 secondes
     ```

- Si un serveur d'applications est sain et qu'aucune durée de suspension n'est requise, la réponse suivante sera alors reçue du healthservlet du serveur :

  ```
  Aucune durée de suspension définie. Code de retour : -1
  ```

6. Configurez la persistance de session sur chaque équilibreur de charge. Ce processus permet de s'assurer qu'une demande provenant d'un serveur d'applications est réacheminée à ce même serveur d'applications.

Vérification des détails de serveur

À l'issue de la configuration, vérifiez que chaque serveur est correctement configuré et disponible.

(pour la Configuration de disponibilité avancée)

1. Vérifiez que tous les serveurs d'arrière-plan, de secours et d'applications sont exécutés.
2. Connectez-vous à l'interface utilisateur Web du serveur d'arrière-plan.
3. Sous l'onglet Administration, sélectionnez Système, Serveurs.

   La page Liste des serveurs s'affiche.
4. Assurez-vous que le champ Configuré contient Oui pour les enregistrements de serveur de secours et d'applications.
5. Si l'option État de l'enregistrement est définie sur Désactivé, modifiez le serveur et définissez-le sur Activé. Si vous changez l'état de l'enregistrement d'un serveur, reconfigurez-le.

   Vous avez bien configuré les serveurs pour la configuration de disponibilité avancée.

   Remarque : Vous pouvez cliquer sur l'une des entrées Hôte local de la page Détail du serveur pour afficher les détails du serveur.

(pour la configuration conventionnelle)

1. Vérifiez que le serveur principal et tous les serveurs secondaires sont en cours d'exécution.
2. Connectez-vous à l'interface utilisateur du serveur principal.
3. Sous l'onglet Administration, sélectionnez Système, Serveurs.

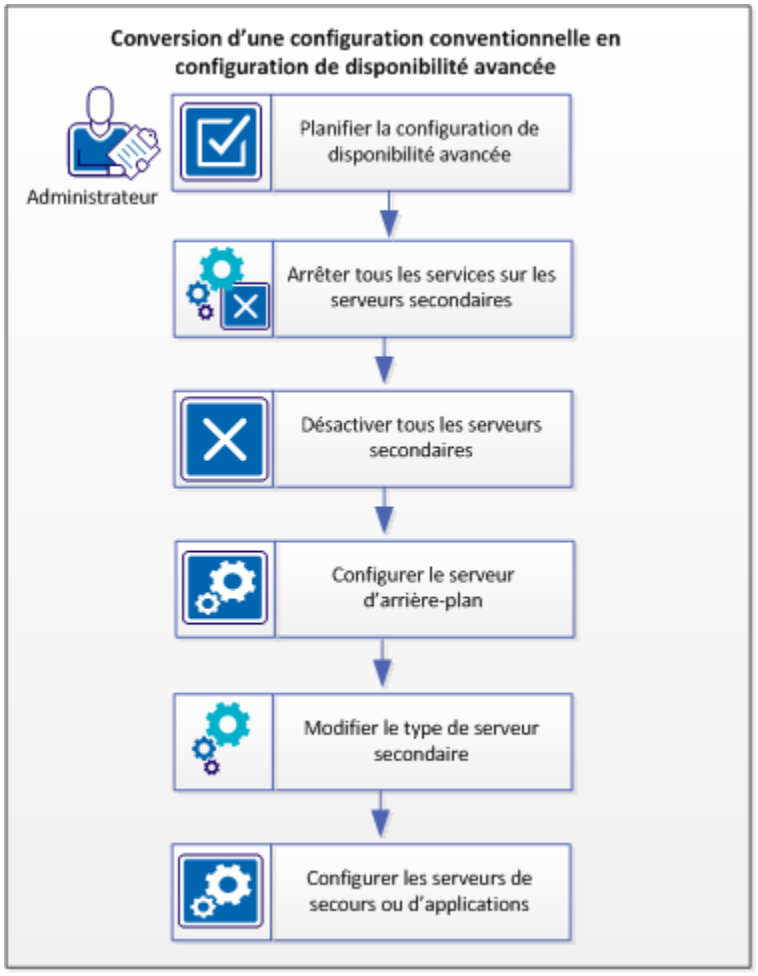
   La page Liste des serveurs s'affiche.
4. Si l'option État de l'enregistrement est définie sur Désactivé, modifiez le serveur et définissez-le sur Activé. Si vous changez l'état de l'enregistrement, veillez à reconfigurer ce serveur.

   Vous avez bien configuré les serveurs.

Procédure de conversion de la configuration conventionnelle en configuration de disponibilité avancée

Avant de convertir la configuration conventionnelle en disponibilité avancée, assurez-vous d'avoir mis à niveau ou installé CA SDM r12.9 sur tous les serveurs.

Le schéma suivant illustre la conversion de la configuration conventionnelle en disponibilité avancée :


Conversion d'une configuration conventionnelle en configuration de disponibilité avancée
Administrateur
Planifier la configuration de disponibilité avancée
Arrêter tous les services sur les serveurs secondaires
Désactiver tous les serveurs secondaires
Configurer le serveur d'arrière-plan
Modifier le type de serveur secondaire
Configurer les serveurs de secours ou d'applications

1. Planifiez la configuration de disponibilité avancée. Pour de plus amples renseignements, consultez le scénario de planification ou le *Manuel de mise en oeuvre*.
2. Arrêtez tous les services sur les serveurs secondaires.
3. Désactivez tous les serveurs secondaires (page 147).

4. Configurez le serveur d'arrière-plan (page 147).
5. Changez le type de serveur secondaire (page 148).
6. Configurez le serveur de secours ou d'applications.
7. Vérifiez les détails du serveur (page 150).

Désactivation de tous les serveurs secondaires

Avant de configurer les serveurs pour la configuration de disponibilité avancée, veillez à désactiver tous les serveurs secondaires.

1. Connectez-vous à l'interface utilisateur Web du serveur principal.
2. Sous l'onglet Administration, sélectionnez Système, Serveurs.

   La page Liste des serveurs s'affiche.
3. Cliquez sur le nom d'hôte du serveur secondaire.

   La page Détail du serveur s'affiche.
4. Cliquez sur Modifier.
5. Définissez l'état de l'enregistrement sur Désactivé.

   Important : Si vous avez désactivé un serveur, il est recommandé de ne pas démarrer de service CA SDM sur ce serveur. Une telle action peut causer un comportement inattendu.
6. Cliquez sur Enregistrer.

   Le serveur secondaire est défini sur Désactivé.
7. Effectuez les étapes 3 à 6 pour tous les autres serveurs secondaires.

   Tous les serveurs secondaires sont définis sur Désactivé.

Configuration du serveur d'arrière-plan

Configurez le serveur d'arrière-plan avant de configurer les serveurs d'applications ou de secours.

1. Connectez-vous au serveur principal.

2. Utilisez la commande pdm_configure pour démarrer la configuration.

   La fenêtre Sélectionner une configuration de serveur s'ouvre.

3. Sélectionnez Disponibilité avancée comme type de configuration et suivez les invites pour réaliser la configuration. Pour de plus amples renseignements, reportez-vous à l'*Aide sur la configuration de serveurs*.

   Le serveur d'arrière-plan est désormais configuré.

Changement du type de serveur secondaire

Une fois le serveur d'arrière-plan configuré, définissez le type de tous les serveurs secondaires sur serveurs d'applications et de secours et activez-les.

1. Assurez-vous que le serveur d'arrière-plan est en cours d'exécution.
2. Connectez-vous à l'interface utilisateur Web du serveur d'arrière-plan.
3. Sous l'onglet Administration, sélectionnez Système, Serveurs.

   La page Liste des serveurs s'affiche.

4. Définissez l'état d'enregistrement de tous les serveurs secondaires sur Activé.
5. Définissez le type de tous les serveurs secondaires en serveurs d'applications ou de secours, comme requis.

   Le type de tous les serveurs secondaires est changé.

Configurez les serveurs de secours et d'applications.

Une fois le serveur d'arrière-plan configuré, configurez chaque serveur de secours et d'applications. Cette configuration est requise pour établir la communication avec le serveur d'arrière-plan.

Important : (Recommandé) Veillez à ce que la configuration du serveur d'arrière-plan et de tous les autres serveurs de secours soit identique. Ce processus permet au serveur de secours de fonctionner comme le serveur d'arrière-plan lors d'un basculement.

1. Connectez-vous au serveur secondaire.
2. Utilisez la commande pdm_configure pour démarrer la configuration.

   La fenêtre Sélectionner une configuration de serveur s'ouvre.

3. Sélectionnez Disponibilité avancée comme type de configuration et suivez les invites pour réaliser la configuration. Pour de plus amples renseignements, reportez-vous à l'*Aide sur la configuration de serveurs*.

4. Répétez les étapes 1 à 3 pour chaque serveur à configurer comme serveur de secours et d'applications.

   Vous avez configuré les serveurs de secours et d'applications.

5. Configurez l'équilibreur de charge (page 144) si vous disposez d'un ou de plusieurs serveurs d'applications et que vous souhaitez l'utiliser pour suivre les demandes à destination et en provenance de différents serveurs d'applications.

   Remarque : Pour utiliser une URL d'équilibreur de charge ou d'un serveur d'applications pour les liens qui se trouvent dans les notifications CA SDM, procédez comme suit :

   a. Connectez-vous au serveur d'arrière-plan.

   b. Sous l'onglet Administration, sélectionnez Gestionnaire d'options, Notifications.

   c. Remplacez la valeur de l'option web_cgi_url afin qu'elle pointe vers les éléments ci-dessous.

      - L'équilibreur de charge, si vous disposez de plusieurs serveurs d'applications.
      - Le serveur d'applications, si vous en avez un seul.

6. Vérification des détails du serveur (page 150).

Configuration de l'équilibreur de charge

Si vous utilisez un ou plusieurs serveurs d'applications, configurez l'équilibrer de changer afin qu'il surveille les serveurs d'applications.

1. Connectez-vous à un serveur d'applications.
2. Copier le fichier HealthServlet.war se trouvant dans le dossier $NX_ROOT/samples/HealthServlet dans le dossier $NX_ROOT/bopcfg/www/CATALINA_BASE/webapps.
3. Redémarrez les services CA SDM ou redémarrez CA SDM Tomcat.
4. Répétez les étapes 1 à 3 pour tous les serveurs d'applications.
5. Configurez l'équilibreur de charge pour qu'il surveille l'URL du healthservlet suivant, sur chacun des serveurs d'applications :

   ```
   http://<Machine_name>:<Port_number>/HealthServlet/GetHealth
   ```

   - Si l'URL du healthservet reçoit une réponse de suspension d'un serveur d'applications, l'équilibreur de charge doit alors rediriger toutes les demandes de ce serveur vers l'autre serveur d'applications. Par exemple, la réponse suivante est reçue lorsque le serveur d'applications est suspendu pendant 58677 secondes.

     ```
     Durée de suspension restante : 58677 secondes
     ```

- Si un serveur d'applications est sain et qu'aucune durée de suspension n'est requise, la réponse suivante sera alors reçue du healthservlet du serveur :

  ```
  Aucune durée de suspension définie. Code de retour : -1
  ```

6. Configurez la persistance de session sur chaque équilibreur de charge. Ce processus permet de s'assurer qu'une demande provenant d'un serveur d'applications est réacheminée à ce même serveur d'applications.

Vérification des détails de serveur

À l'issue de la configuration, vérifiez que chaque serveur est correctement configuré et disponible.

1. Vérifiez que tous les serveurs d'arrière-plan, de secours et d'applications sont exécutés.
2. Connectez-vous à l'interface utilisateur Web du serveur d'arrière-plan.
3. Sous l'onglet Administration, sélectionnez Système, Serveurs.

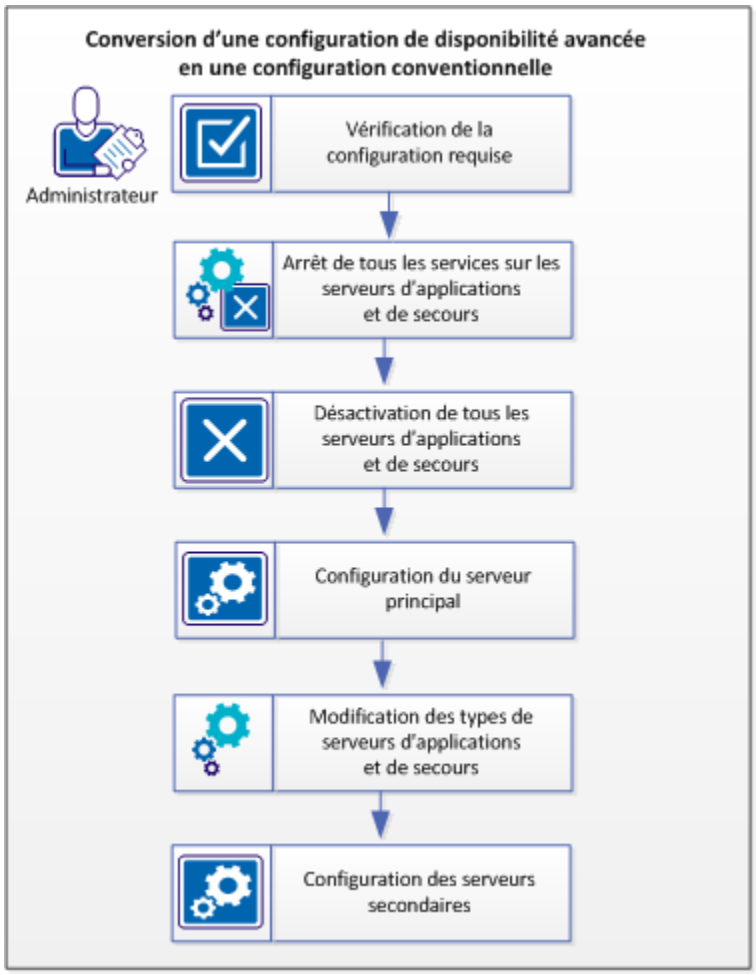
   La page Liste des serveurs s'affiche.
4. Assurez-vous que le champ Configuré contient Oui pour les enregistrements de serveur de secours et d'applications.
5. Si l'option État de l'enregistrement est définie sur Désactivé, modifiez le serveur et définissez-le sur Activé. Si vous changez l'état de l'enregistrement d'un serveur, reconfigurez-le.

   Vous avez bien configuré les serveurs pour la configuration de disponibilité avancée.

   Remarque : Vous pouvez cliquer sur l'une des entrées Hôte local de la page Détail du serveur pour afficher les détails du serveur.

Procédure de conversion de la configuration de disponibilité avancée en conventionnelle

Vous pouvez revenir à la configuration conventionnelle à partir de la configuration de disponibilité avancée. Le schéma suivant illustre la conversion de la configuration de disponibilité avancée en conventionnelle :


Conversion d'une configuration de disponibilité avancée en une configuration conventionnelle
Administrateur
Vérification de la configuration requise
Arrêt de tous les services sur les serveurs d'applications et de secours
Désactivation de tous les serveurs d'applications et de secours
Configuration du serveur principal
Modification des types de serveurs d'applications et de secours
Configuration des serveurs secondaires

1. Vérifiez la configuration requise. (page 152)
2. Stoppez tous les services sur les serveurs d'applications et de secours.
3. Désactivez tous les serveurs d'applications et de secours (page 152).
4. Configurez le serveur principal (page 140).

5. Changez les types des serveurs d'applications et de secours (page 153).
6. Configurez les serveurs secondaires (page 142).
7. Vérification des détails de serveur (page 154)

Vérifiez la configuration requise.

Avant d'effectuer la conversion vers la configuration conventionnelle, vérifiez que les conditions suivantes sont réunies :

1. Vous avez planifié la configuration conventionnelle. Pour de plus amples renseignements, consultez le chapitre sur la planification dans le *Manuel de mise en oeuvre*.
2. Vous pouvez uniquement configurer le serveur d'arrière-plan comme serveur principal.
3. Vous pouvez uniquement configurer les serveurs de secours et d'applications comme serveurs secondaires.

Désactivation de tous les serveurs d'applications et de secours

Avant de configurer les serveurs pour la configuration conventionnelle, veillez à désactiver tous les serveurs d'applications et de secours.

1. Connectez-vous à l'interface utilisateur Web du serveur d'arrière-plan.
2. Sous l'onglet Administration, sélectionnez Système, Serveurs.

   La page Liste des serveurs s'affiche.
3. Cliquez sur le nom d'hôte du serveur d'applications.

   La page Détail du serveur s'affiche.
4. Cliquez sur Modifier.
5. Définissez l'état de l'enregistrement sur Désactivé.

Important : Si vous avez désactivé un serveur, il est recommandé de ne pas démarrer de service CA SDM sur ce serveur. Une telle action peut causer un comportement inattendu.

6. Cliquez sur Enregistrer.

   Le serveur d'applications est défini sur Désactivé.

7. Effectuez les étapes 3 à 6 pour tout autre serveur d'applications et de secours.

   Tous les serveurs d'applications et de secours sont définis sur Désactivé.

Configuration du serveur principal

Le serveur principal doit être configuré avant que vous ne puissiez configurer de serveurs secondaires.

1. Connectez-vous à l'interface utilisateur Web du serveur d'arrière-plan.
2. Utilisez l'interface utilisateur Web du serveur d'arrière-plan pour désactiver le serveur d'arrière-plan.
3. Utilisez la commande pdm_configure pour démarrer la configuration.

   La fenêtre Sélectionner une configuration de serveur s'ouvre.

4. Sélectionnez Conventionnelle comme type de configuration et suivez les invites pour réaliser la configuration. Pour de plus amples renseignements, reportez-vous à l'*Aide sur la configuration de serveurs*.

   Le serveur principal est désormais configuré.

Vérification des détails du serveur

Une fois le serveur principal configuré, définissez le type de tous les serveurs d'applications et de secours en serveurs secondaires, puis activez-les.

1. Assurez-vous que le serveur principal est en cours d'exécution.
2. Connectez-vous à l'interface utilisateur du serveur principal.
3. Sous l'onglet Administration, sélectionnez Système, Serveurs.

   La page Liste des serveurs s'affiche.

4. Définissez l'état de l'enregistrement pour tous les serveurs d'applications et de secours sur Activé.
5. Changez le type de tous les serveurs d'applications et de secours en serveurs secondaires.

   Le type de tous les serveurs d'applications et de secours est changé.

Configuration des serveurs secondaires

Vous configurerez chacun des serveurs secondaires après avoir configuré le serveur principal. Cette configuration est requise pour établir la communication avec le serveur principal.

1. Connectez-vous au serveur d'applications ou au serveur de secours que vous voulez configurer comme nouveau serveur secondaire.
2. Utilisez la commande pdm_configure pour démarrer la configuration.

   La fenêtre Sélectionner une configuration de serveur s'ouvre.
3. Sélectionnez Conventionnelle comme type de configuration et suivez les invites pour réaliser la configuration. Pour de plus amples renseignements, reportez-vous à l'*Aide sur la configuration de serveurs*.

   Le serveur secondaire est désormais configuré.
4. Répétez les étapes 1 à 3 sur chaque serveur à configurer comme serveur secondaire.

Vérification des détails de serveur

À l'issue de la configuration, vérifiez que chaque serveur est correctement configuré et disponible.

1. Vérifiez que le serveur principal et tous les serveurs secondaires sont en cours d'exécution.
2. Connectez-vous à l'interface utilisateur du serveur principal.
3. Sous l'onglet Administration, sélectionnez Système, Serveurs.

   La page Liste des serveurs s'affiche.
4. Si l'option État de l'enregistrement est définie sur Désactivé, modifiez le serveur et définissez-le sur Activé. Si vous changez l'état de l'enregistrement, veillez à reconfigurer ce serveur.

   Vous avez bien configuré les serveurs.

Installation de la CA MDB

Remarque : Avant d'installer ce composant, assurez-vous d'avoir planifié l'installation de la CA MDB (page 99).

Important : Le mappage de l'image de DVD à l'aide d'un chemin d'accès UNC n'est pas pris en charge par le programme d'installation de la CA MDB.

Si la base de données (SQL Server ou Oracle) que vous voulez utiliser avec CA SDM est installée sur un serveur autre que le serveur principal CA SDM, installez manuellement la CA MDB sur le serveur de base de données distant (c'est-à-dire, l'ordinateur sur lequel est installé SQL Server ou Oracle). Si le serveur principal et la CA MDB sont sur le même ordinateur, il n'est pas nécessaire d'installer la CA MDB manuellement. CA SDM installe automatiquement la CA MDB pendant l'installation de CA SDM.

Remarque : Si vous voulez installer la base de données de gestion sur le serveur principal, vous *devez* démarrer et exécuter l'installation de la CA MDB sur l'ordinateur distant qui héberge le serveur de base de données.

Installations de MDB

Pour les installations de MDB, les conditions suivantes s'appliquent :

- Quand vous effectuez une Installation de MDB pour installer la base de données SQL sur un serveur différent, le client natif SQL ainsi que les outils client et de gestion doivent être installés sur le client CA CMDB.
- Pour toute configuration de base de données Oracle, le logiciel client Oracle doit également être installé. Vous pouvez télécharger le logiciel client Oracle depuis le site Web d'Oracle.

Rechercher des informations sur l'intégration et la compatibilité des produit

Consultez les informations fournies par le service de soutien de CA pour connaître la compatibilité entre CA MDB et CA SDM et d'autres produits.

- *CA Service Accounting and CA Service Catalog Integration Guide* : décrit les versions de CA MDB et explique comment déterminer si vous devez installer un correctif de compatibilité avec CA MDB afin que d'autres produits puissent être intégrés à CA MDB.
- *CA Management Database Mixed Version Installation* : décrit la compatibilité avec CA MDB.

Pour trouver des informations sur l'intégration à CA MDB

1. Ouvrez un navigateur et accédez au site http://support.ca.com.

   La page Service de soutien CA s'affiche.

2. Connectez-vous au service de soutien CA.

3. Cliquez sur le lien Documentation dans le volet gauche.

   La page Documentation s'affiche.

4. Dans les listes déroulantes, sélectionnez CA Service Catalog r12 et English US. Cliquez sur OK.

   La liste de documentation de CA Service Catalog s'affiche.

5. Cliquez sur le lien PDF pour accéder au document intitulé Integration Guide J02775-1E

   Le manuel *CA Service Accounting and CA Service Catalog Integration Guide* s'affiche.

6. Cliquez sur le signet permettant d'activer l'intégration avec les produits CA qui utilisent une version antérieure de la base de données.

   Ces informations sont fournies pour vous aider à intégrer des produits à CA MDB.

Pour trouver des informations sur la compatibilité

1. Ouvrez un navigateur et accédez au site http://support.ca.com.

   La page Service de soutien CA s'affiche.

2. Connectez-vous au service de soutien CA.

3. Dans le volet Soutien, cliquez sur Recherche dans la base de connaissances.

   La page Recherche dans la base de connaissances s'affiche.

4. Entrez **MDB104 Compatibility** (Compatibilité MDB104) dans le champ de recherche. Cliquez sur Rechercher.

   Les résultats de la recherche dans la base de connaissances s'affichent.

5. Cliquez sur le lien permettant d'installer une version mixte de la base de données de gestion de CA.

   Le document *CA Management Database Mixed Version Installation* s'affiche.

Installation sur SQL Server (Windows)

Si vous utilisez la configuration de disponibilité avancée et que la CA MDB utilisée est installée sur un ordinateur différent du serveur CA SDM, vous devez installer la CA MDB sur le serveur de base de données distant, c'est-à-dire, l'ordinateur sur lequel SQL Server est installé.

1. Insérez le support d'installation dans votre lecteur.

   Important : Si votre ordinateur ne dispose pas d'un lecteur approprié pour le support d'installation, copiez le contenu du support sur l'ordinateur sur lequel vous souhaitez installer CA SDM. Puis, démarrez l'installation. Pour une installation distante sur le réseau, vous pouvez partager un lecteur ou un dossier sur le réseau, puis vous connecter par l'entremise du réseau pour démarrer l'installation.

2. Pour sélectionner votre langue dans la liste, cliquez sur Sélectionner une langue.

   Le menu d'installation s'affiche.

   Remarque : Si le menu Installation ne s'affiche pas automatiquement, démarrez l'installation en double-cliquant sur le fichier setup.exe, situé à la racine du support d'installation.

3. Cliquez sur l'onglet Installer le produit.

4. Cliquez sur la CA MDB.

5. Suivez les instructions à l'écran pour poursuivre l'installation.

6. À l'invite, sélectionnez SQL Server comme type de la base de données et entrez les renseignements appropriés pour SQL Server.

   Remarque : Si vous ne savez pas quelles données entrer pour SQL Server, reportez-vous à l'*Aide en ligne relative à la configuration du serveur*.

7. Continuez de suivre les instructions à l'écran pour terminer l'installation de la CA MDB.

   La CA MDB est installée sur SQL Server.

Renseignements supplémentaires :

Fichier journal d'installation (page 236)

Installation sur Oracle (Windows)

Si vous utilisez la configuration de disponibilité avancée et que la CA MDB utilisée est installée sur un ordinateur différent du serveur CA SDM, vous devez installer la CA MDB sur le serveur de base de données distant, c'est-à-dire, l'ordinateur sur lequel SQL Server est installé.

1. Insérez le support d'installation dans votre lecteur.

   Important : Si votre ordinateur ne dispose pas d'un lecteur approprié pour le support d'installation, copiez le contenu du support sur l'ordinateur sur lequel vous souhaitez installer CA SDM. Puis, démarrez l'installation. Pour une installation distante sur le réseau, vous pouvez partager un lecteur ou un dossier sur le réseau, puis vous connecter par l'entremise du réseau pour démarrer l'installation.

   Le menu d'installation s'affiche.

   Remarque : Si le menu Installation ne s'affiche pas automatiquement, démarrez l'installation en double-cliquant sur le fichier setup.exe, situé à la racine du support d'installation.

2. Cliquez sur l'onglet Installer le produit.
3. Cliquez sur la CA MDB.
4. Suivez les instructions à l'écran pour poursuivre l'installation.
5. À l'invite, sélectionnez Oracle comme type de la base de données et entrez les renseignements appropriés pour Oracle.

   Remarque : Si vous ne savez pas quelles données entrer pour Oracle, reportez-vous à l'*Aide en ligne relative à la configuration du serveur*.

6. Entrez et sélectionnez les renseignements pour configurer la base de données Oracle.

   CA SDM requiert un nom de service Net qui spécifie la base de données Oracle où réside la MDB. CA SDM requiert également un identificateur de système (SID) pour la base de données. Ces noms peuvent être différents, même s'ils spécifient la même base de données MDB. Deux valeurs de nom sont requises pour CA SDM car il accède à la base de données avec à la fois la technologie cliente d'Oracle et la technologie JDBC.

   Remarque : Pour de plus amples renseignements sur les noms de services et les identificateurs de système, reportez-vous à la documentation d'Oracle.

Charger les données par défaut

Spécifie si les données CA SDM par défaut sont chargées dans la base de données Oracle.

Si cette case est cochée, le système charge les données système par défaut de CA SDM dans la base de données Oracle. Si vous avez modifié des valeurs système par défaut, cette option remplace les valeurs. Sélectionnez cette case à cocher pour les premières installations. Cette option remplace les données existantes lorsqu'il ne s'agit pas d'une première installation. Si cette case n'est pas cochée, aucune donnée par défaut n'est chargée.

Base de données distante

Indique qu'une base de données Oracle est installée sur un serveur autre que le serveur principal CA SDM. Installez manuellement CA MDB sur le serveur de base de données distant (c'est-à-dire, l'ordinateur sur lequel Oracle est installé) avant d'installer CA SDM.

Si le serveur Oracle est local (non sélectionné), CA SDM crée la MDB si elle ne l'est pas encore.

Créer des espaces disque logiques

Spécifie s'il faut créer des espaces disque logiques pour la base de données MDB ou utiliser les espaces disque logiques déjà créés.

- Désélectionnez cette case à cocher si vous avez déjà créé des espaces disque logiques manuellement. Fournissez les noms des espaces disque logiques existants. Le champ du chemin d'accès à l'espace disque logique dans le produit est désactivé et les champs Nom de l'espace disque logique de données et Nom de l'espace disque logique d'index sont activés.
- Sélectionnez cette case à cocher pour créer des espaces disque logiques avec les noms MDB_DATA et MDB_INDEX par défaut. Fournissez un chemin d'accès à l'espace disque logique. Les champs Nom de l'espace disque logique de données et Nom de l'espace disque logique d'index sont désactivés.

Remarque : Si vous utilisez Oracle Automated Storage Manager (ASM), créez manuellement un espace disque logique Oracle avant d'installer CA SDM. Lorsqu'Oracle est installé et configuré pour ASM, nous ne pouvons pas créer un espace disque logique Oracle pendant notre installation de MDB. ASM utilise le stockage virtuel et nous recherchons un répertoire physique. Par conséquent, nous ne pouvons pas créer correctement l'espace disque logique avec cette configuration.

Nom du service Net

Indique le nom du service Net de la base de données Oracle où se trouve la MDB. Si la base de données est distante, utilisez le nom du service Net défini dans le client Oracle sur l'ordinateur local. CA SDM accède à la base de données à l'aide d'une installation locale du client Oracle, qui peut spécifier un nom de service Net différent de celui indiqué sur le serveur Oracle.

Mot de passe de l'utilisateur mdbadmin

Spécifie le mot de passe de l'utilisateur mdbadmin. Fournissez le mot de passe existant ou spécifiez-en un nouveau si CA SDM crée l'utilisateur.

Nom de l'utilisateur DBA

Spécifie le nom d'un utilisateur d'Oracle avec un accès DBA (généralement SYS). Ce champ est utilisé uniquement si le serveur Oracle se trouve sur l'ordinateur local.

Mot de passe DBA

Indique le mot de passe de l'utilisateur DBA. Ce champ est utilisé uniquement si le serveur Oracle se trouve sur l'ordinateur local.

Nom de l'espace disque logique de données

Crée le nom de l'espace disque logique de données spécifié lorsque la case Créer des espaces disque logiques est cochée. Ce champ est utilisé uniquement si le serveur Oracle se trouve sur l'ordinateur local.

Nom de l'espace disque logique d'index

Crée le nom de l'espace disque logique d'index spécifié lorsque la case Créer des espaces disque logiques est cochée. Ce champ est utilisé uniquement si le serveur Oracle se trouve sur l'ordinateur local.

Chemin d'accès à l'espace disque logique

Spécifie le chemin d'accès du répertoire à l'emplacement de l'espace disque logique physique créé si les espaces disque logiques précédemment mentionnés n'existent pas. Ce champ est utilisé uniquement si le serveur Oracle se trouve sur l'ordinateur local.

Chemin d'accès au répertoire d'installation d'Oracle

Spécifie le chemin d'accès du répertoire au chemin d'accès du répertoire d'installation d'Oracle

Connectivité JDBC

Spécifie si la connectivité JDBC doit être utilisée. Plusieurs composants de CA SDM utilisent la technologie JDBC pour accéder à la base de données et requièrent des renseignements spécifiques à propos du serveur Oracle.

Identifiez le nom d'hôte de la base de données, l'ID de système et le port d'écouteur configurés précédemment.

La CA MDB est installée sur Oracle.

Renseignements supplémentaires :

Fichier journal d'installation (page 236)

Installation sur Oracle (Linux\UNIX)

Si vous utilisez la configuration de disponibilité avancée et que la CA MDB utilisée est installée sur un ordinateur différent du serveur CA SDM, vous devez installer la CA MDB sur le serveur de base de données distant, c'est-à-dire, l'ordinateur sur lequel SQL Server est installé.

Remarque : Vérifiez que votre environnement Oracle est correctement configuré et accessible.

1. Montez le support d'installation sur votre lecteur.

   Important : Si votre ordinateur ne dispose pas d'un lecteur approprié pour le support d'installation, copiez le contenu du support sur l'ordinateur sur lequel vous souhaitez installer CA SDM. Puis, démarrez l'installation. Pour une installation distante sur le réseau, vous pouvez partager un lecteur ou un dossier sur le réseau, puis vous connecter par l'entremise du réseau pour démarrer l'installation.

2. Accédez au répertoire racine du support d'installation et démarrez l'installation en exécutant la commande suivante :

   ```
   sh ./setup.sh
   ```

3. Pour sélectionner votre langue dans la liste, cliquez sur Sélectionner une langue.

   Le menu d'installation s'affiche.

4. Cliquez sur l'onglet Installer le produit.

5. Cliquez sur la CA MDB.

6. Suivez les instructions à l'écran pour poursuivre l'installation.

7. À l'invite, sélectionnez Oracle comme type de la base de données et entrez les renseignements appropriés pour Oracle.

   Remarque : Si vous ne savez pas quelles données entrer pour Oracle, reportez-vous à l'*Aide en ligne relative à la configuration du serveur*.

8. Continuez de suivre les instructions à l'écran pour terminer l'installation de la CA MDB.

   La CA MDB est installée sur Oracle.

Renseignements supplémentaires :

Fichier journal d'installation (page 236)

Installation d'une MDB distante sous HP-UX

Vous pouvez installer une MDB distante sous HP-UX.

1. Téléchargez le programme d'installation de la CA MDB pour HP-UX à partir du portail de soutien de CA ou contactez le soutien technique de CA pour obtenir ce programme.
2. Décompressez le média à l'emplacement de votre choix.
3. Vérifiez que le dossier de la CA MDB dispose de toutes les autorisations pour tous les utilisateurs.

   Par exemple : chmod -R 777 mdb.

4. Accédez au dossier Oracle et exécutez la commande suivante :

   ```
   ./setupmdb.sh -DBVENDOR=oracle -DBHOST=<DBHOST_NAME> -DBNAME=<ORACLE_SID>
   -DBUSER=<DB_User_SYS_name> -DBPASSWORD=<DB_User_SYS_password>
   -MDB_ADMIN_PSWD=<MDB_ADMIN_PASSWORD>
   -ORA_TBLSPACE_PATH=<Oralce_Table_Space_path> -MANIFEST=Service_Desk
   -WORKSPACE=Service_Desk -JRE_DIR=<JRE_PATH> -MDB_COMMON_DIR=<mdb_Common_DIR>
   ```

5. Par exemple, exécutez la commande suivante :

   ```
   ./setupmdb.sh -DBVENDOR=oracle -DBHOST=hostname -DBNAME=mdb -DBUSER=SYS
   -DBPASSWORD=mdbpassword -MDB_ADMIN_PSWD=mdbpassword
   -ORA_TBLSPACE_PATH=/sdhome/oracle/oracle/product/10,2.0/db_1/oradata/mdb
   -MANIFEST=Service_Desk -WORKSPACE=Service_Desk
   -JRE_DIR=/sdhome/opt/Sharedcomponents/JRE/1.6,0_00
   -MDB_COMMON_DIR=/sdhome/opt/Sharedcomponents/Mdb
   ```

   L'installation de la CA MDB est terminée et un message s'affiche, indiquant la correcte installation.

Installation de CA SDM

Remarque : Avant d'installer ce composant, assurez-vous d'avoir planifié l'installation de CA SDM (page 102). En outre, quand vous réalisez une installation sous Linux et UNIX, certains messages contextuels ne s'affichent pas clairement si vos propriétés de couleur sont blanc sur blanc.

Lorsque vous démarrez et installez CA SDM sur un serveur, les fichiers, les composants et les fonctionnalités qui suivent sont installés pour l'utilisation du produit :

- Fonction du serveur, selon votre configuration du produit à l'issue de l'installation
- Interface SQL Server ou Oracle
- Interface ODBC

  Important : L'installation de l'interface ODBC doit uniquement être utilisée pour accéder au pilote ODBC pour le signalement BusinessObjects dans CA SDM avec CA Business Intelligence. L'utilisation du pilote ODBC par d'autres applications n'est pas directement prise en charge, certifiée ou garantie par CA Technologies et vous devez en assumer l'entière responsabilité.
- Interface Web
- CA CMDB

  Important : Pendant la configuration, lorsque vous migrez de la version autonome de CA CMDB vers CA SDM, une case à cocher Configurer uniquement CA CMDB s'affiche. Lorsque vous désactivez la case à cocher Configurer uniquement CA CMDB et que vous cliquez sur Suivant, vous ne pouvez pas configurer CA CMDB à nouveau. Même si vous cliquez sur Retour, la case à cocher Configurer uniquement CA CMD n'est plus disponible. Un message vous avertit de ce comportement dans la boîte de dialogue de configuration. Si vous annulez la configuration avant la fin et la reprenez, la case à cocher Configurer uniquement CA CMD est disponible.

  La case à cocher Configurer uniquement CA CMD contrôle la valeur de la variable d'environnement CA SDM NX_CMDB. La variable d'environnement contrôle si la fonctionnalité Automatisation du soutien est configurée. Si la case à cocher est désactivée, la fonctionnalité Automatisation du soutien est configurable, sinon il ne l'est pas. La variable d'environnement affecte le comportement de certains formulaires Web.
- Visualiseur
- Automatisation du soutien

  Installez l'option *supportautomation_url* après avoir configuré Automatisation du soutien pendant la configuration de CA SDM. Pour de plus amples renseignements sur cette option, reportez-vous à l'*Aide en ligne*.

Important : Lorsque vous désinstallez CA SDM, CA Workflow est également désinstallé.

Variables de l'environnement Oracle

Avant d'installer ou d'effectuer une migration CA SDM, définissez les variables d'environnement Oracle comme suit :

- Vérifiez que la variable ORACLE_HOME est correctement définie.

  Important : Vous devez exporter la variable TWO_TASK lorsque les variables clientes 32 bits Oracle sont exportées sur une plate-forme différente de Windows.

- Incluez les bibliothèques Oracle 32 bits (généralement, $ORACLE_HOME/lib32 pour Oracle 64 bits) dans la variable de chemin d'accès à la bibliothèque LD_LIBRARY_PATH (LIBPATH sous AIX).

Installation sur SQL Server (Windows)

Lorsque vous démarrez et installez CA SDM sur un serveur, les composants et fonctionnalités qui suivent sont installés :

- Fonction du serveur, selon votre configuration du produit à l'issue de l'installation
- Interface SQL Server
- Interface Web
- Interface ODBC

Important : L'installation de l'interface ODBC doit uniquement être utilisée pour accéder au pilote ODBC pour le signalement BusinessObjects dans CA SDM avec CA Business Intelligence. L'utilisation du pilote ODBC par d'autres applications n'est pas directement prise en charge, certifiée ou garantie par CA Technologies et vous devez en assumer l'entière responsabilité.

1. Insérez le support d'installation dans votre lecteur.

   Important : Si votre ordinateur ne dispose pas d'un lecteur approprié pour le support d'installation, copiez le contenu du support sur l'ordinateur sur lequel vous souhaitez installer CA SDM. Puis, démarrez l'installation. Pour une installation distante sur le réseau, vous pouvez partager un lecteur ou un dossier sur le réseau, puis vous connecter par l'entremise du réseau pour démarrer l'installation.

2. Pour sélectionner votre langue dans la liste, cliquez sur Sélectionner une langue.

   Le menu d'installation s'affiche.

   Remarque : Si le menu Installation ne s'affiche pas automatiquement, démarrez l'installation en double-cliquant sur le fichier setup.exe, situé à la racine du support d'installation.

3. Cliquez sur l'onglet Installer le produit.

4. Cliquez sur CA SDM.

5. Pour poursuivre l'installation, suivez les instructions à l'écran.

   L'Assistant de configuration s'affiche.

   Remarque : Si les hôtes Internet Protocol version 4 (IPv4) et Internet Protocol version 6 (IPv6) coexistent sur le réseau, vérifiez que les stratégies de transition, outils et mécanismes appropriés pour prendre en charge ces technologies sont installés avant de démarrer la configuration du produit. Pour de plus amples renseignements sur la configuration des serveurs, reportez-vous au *Manuel d'administration*.

6. Entrez et sélectionnez les renseignements nécessaires à la configuration du produit.

   Remarque : Pour de plus amples renseignements sur les champs qui s'affichent dans l'assistant, reportez-vous à l'*Aide en ligne*.

7. Suivez ensuite les instructions à l'écran pour terminer l'installation.

   CA SDM est installé sur SQL Server.

8. Après la configuration de l'installation, l'assistant fournit des instructions pour le téléchargement et l'exécution du fichier pslist.exe. Suivez ces étapes et cliquez sur Suivant.

9. Après avoir installé CA SDM (ou migré vers CA SDM à partir d'un système autonome CA CMDB), exécutez l'utilitaire *cmdb_update_ambiguity*. Utilisez la commande -h pour afficher les options obligatoires. Pour plus d'informations sur le calcul de l'index d'ambiguïté, consultez le *Manuel d'administration*.

Remarque : Si la configuration échoue lors de l'étape de validation des tables d'extension, la connectivité de la base de données peut poser problème. Exécutez à nouveau la configuration et vérifiez que vous avez fourni les informations de connectivité de la base de données appropriées.

Installation sur Oracle (Windows)

Lorsque vous démarrez et installez CA SDM sur un serveur, les composants et fonctionnalités qui suivent sont installés :

- Fonction du serveur, selon votre configuration du produit à l'issue de l'installation
- Interface Oracle
- Interface Web
- Interface ODBC

Vous devez être l'administrateur pour installer CA MDB ou CA SDM.

Important : L'installation de l'interface ODBC doit uniquement être utilisée pour accéder au pilote ODBC pour le signalement BusinessObjects dans CA SDM avec CA Business Intelligence. L'utilisation du pilote ODBC par d'autres applications n'est pas directement prise en charge, certifiée ou garantie par CA Technologies et vous devez en assumer l'entière responsabilité.

1. Insérez le support d'installation dans votre lecteur.

   Important : Si votre ordinateur ne dispose pas d'un lecteur approprié pour le support d'installation, copiez le contenu du support sur l'ordinateur sur lequel vous souhaitez installer CA SDM. Puis, démarrez l'installation. Pour une installation distante sur le réseau, vous pouvez partager un lecteur ou un dossier sur le réseau, puis vous connecter par l'entremise du réseau pour démarrer l'installation.

2. Pour sélectionner votre langue dans la liste, cliquez sur Sélectionner une langue.

   Le menu d'installation s'affiche.

   Remarque : Si le menu Installation ne s'affiche pas automatiquement, démarrez l'installation en double-cliquant sur le fichier setup.exe, situé à la racine du support d'installation.

3. Cliquez sur l'onglet Installer le produit.

4. Cliquez sur CA SDM.

5. Pour poursuivre l'installation, suivez les instructions à l'écran.

   L'Assistant de configuration s'affiche.

   Remarque : Si les hôtes Internet Protocol version 4 (IPv4) et Internet Protocol version 6 (IPv6) coexistent sur le réseau, vérifiez que les stratégies de transition, outils et mécanismes appropriés pour prendre en charge ces technologies sont installés avant de démarrer la configuration du produit. Pour de plus amples renseignements sur la configuration des serveurs, reportez-vous au *Manuel d'administration*.

6. Entrez et sélectionnez les renseignements pour configurer la base de données Oracle.

   CA SDM requiert un nom de service Net qui spécifie la base de données Oracle où réside la MDB. CA SDM requiert également un identificateur de système (SID) pour la base de données. Ces noms peuvent être différents, même s'ils spécifient la même base de données MDB. Deux valeurs de nom sont requises pour CA SDM car il accède à la base de données avec à la fois la technologie cliente d'Oracle et la technologie JDBC.

   Remarque : Pour de plus amples renseignements sur les noms de services et les identificateurs de système, reportez-vous à la documentation d'Oracle.

   Charger les données par défaut

   Spécifie si les données CA SDM par défaut sont chargées dans la base de données Oracle.

   Si cette case est cochée, le système charge les données système par défaut de CA SDM dans la base de données Oracle. Si vous avez modifié des valeurs système par défaut, cette option remplace les valeurs. Sélectionnez cette case à cocher pour les premières installations. Cette option remplace les données existantes lorsqu'il ne s'agit pas d'une première installation. Si cette case n'est pas cochée, aucune donnée par défaut n'est chargée.

   Base de données distante

   Indique qu'une base de données Oracle est installée sur un serveur distant. Installez manuellement CA MDB sur le serveur de base de données distant (c'est-à-dire, l'ordinateur sur lequel Oracle est installé) avant d'installer CA SDM.

   Si le serveur Oracle est local (non sélectionné), CA SDM crée la MDB si elle ne l'est pas encore.

   Créer des espaces disque logiques

   Spécifie s'il faut créer des espaces disque logiques pour la base de données MDB ou utiliser les espaces disque logiques déjà créés.

   - Désélectionnez cette case à cocher si vous avez déjà créé des espaces disque logiques manuellement. Fournissez les noms des espaces disque logiques existants. Le champ du chemin d'accès à l'espace disque logique dans le produit est désactivé et les champs Nom de l'espace disque logique de données et Nom de l'espace disque logique d'index sont activés.
   - Sélectionnez cette case à cocher pour créer des espaces disque logiques avec les noms MDB_DATA et MDB_INDEX par défaut. Fournissez un chemin d'accès à l'espace disque logique. Les champs Nom de l'espace disque logique de données et Nom de l'espace disque logique d'index sont désactivés.

Remarque : Si vous utilisez Oracle Automated Storage Manager (ASM), créez manuellement un espace disque logique Oracle avant d'installer CA SDM. Lorsqu'Oracle est installé et configuré pour ASM, nous ne pouvons pas créer un espace disque logique Oracle pendant notre installation de MDB. ASM utilise le stockage virtuel et nous recherchons un répertoire physique. Par conséquent, nous ne pouvons pas créer correctement l'espace disque logique avec cette configuration.

Nom du service Net

Indique le nom du service Net de la base de données Oracle où se trouve la MDB. Si la base de données est distante, utilisez le nom du service Net défini dans le client Oracle sur l'ordinateur local. CA SDM accède à la base de données à l'aide d'une installation locale du client Oracle, qui peut spécifier un nom de service Net différent de celui indiqué sur le serveur Oracle.

Mot de passe de l'utilisateur mdbadmin

Spécifie le mot de passe de l'utilisateur mdbadmin. Fournissez le mot de passe existant ou spécifiez-en un nouveau si CA SDM crée l'utilisateur.

Nom de l'utilisateur DBA

Spécifie le nom d'un utilisateur d'Oracle avec un accès DBA (généralement SYS). Ce champ est utilisé uniquement si le serveur Oracle se trouve sur l'ordinateur local.

Mot de passe DBA

Indique le mot de passe de l'utilisateur DBA. Ce champ est utilisé uniquement si le serveur Oracle se trouve sur l'ordinateur local.

Nom de l'espace disque logique de données

Crée le nom de l'espace disque logique de données spécifié lorsque la case Créer des espaces disque logiques est cochée. Ce champ est utilisé uniquement si le serveur Oracle se trouve sur l'ordinateur local.

Nom de l'espace disque logique d'index

Crée le nom de l'espace disque logique d'index spécifié lorsque la case Créer des espaces disque logiques est cochée. Ce champ est utilisé uniquement si le serveur Oracle se trouve sur l'ordinateur local.

Chemin d'accès à l'espace disque logique

Spécifie le chemin d'accès du répertoire à l'emplacement de l'espace disque logique physique créé si les espaces disque logiques précédemment mentionnés n'existent pas. Ce champ est utilisé uniquement si le serveur Oracle se trouve sur l'ordinateur local.

Chemin d'accès au répertoire d'installation d'Oracle

Spécifie le chemin d'accès du répertoire au chemin d'accès du répertoire d'installation d'Oracle

Connectivité JDBC

Spécifie si la connectivité JDBC doit être utilisée. Plusieurs composants de CA SDM utilisent la technologie JDBC pour accéder à la base de données et requièrent des renseignements spécifiques à propos du serveur Oracle.

Identifiez le nom d'hôte de la base de données, l'ID de système et le port d'écouteur configurés précédemment.

7. Suivez ensuite les instructions à l'écran pour terminer l'installation.

   CA SDM est installé sur Oracle.

8. Après la configuration de l'installation, l'assistant fournit des instructions pour le téléchargement et l'exécution du fichier pslist.exe. Suivez ces étapes et cliquez sur Suivant.

9. Après avoir installé CA SDM (ou migré vers CA SDM à partir d'un système autonome CA CMDB), exécutez l'utilitaire *cmdb_update_ambiguity*. Utilisez la commande -h pour afficher les options obligatoires. Pour plus d'informations sur le calcul de l'index d'ambiguïté, consultez le *Manuel d'administration*.

Installation sur Oracle (Linux\UNIX)

Lorsque vous démarrez et installez CA SDM sur un serveur, les composants et fonctionnalités qui suivent sont installés :

- Fonction du serveur, selon votre configuration du produit à l'issue de l'installation
- Interface Oracle
- Interface Web
- Interface ODBC

Important : L'installation de l'interface ODBC doit uniquement être utilisée pour accéder au pilote ODBC pour le signalement BusinessObjects dans CA SDM avec CA Business Intelligence. L'utilisation du pilote ODBC par d'autres applications n'est pas directement prise en charge, certifiée ou garantie par CA Technologies et vous devez en assumer l'entière responsabilité.

Remarque : Vérifiez que votre environnement Oracle est correctement configuré et accessible.

1. Montez le support d'installation sur votre lecteur.

   Important : Si votre ordinateur ne dispose pas d'un lecteur approprié pour le support d'installation, copiez le contenu du support sur l'ordinateur sur lequel vous souhaitez installer CA SDM. Puis, démarrez l'installation. Pour une installation distante sur le réseau, vous pouvez partager un lecteur ou un dossier sur le réseau, puis vous connecter par l'entremise du réseau pour démarrer l'installation.

2. Accédez au répertoire racine du support d'installation et démarrez l'installation en exécutant la commande suivante :

   ```
   sh ./setup.sh
   ```

3. Pour sélectionner votre langue dans la liste, cliquez sur Sélectionner une langue.

   Le menu d'installation s'affiche.

   Remarque : En cas d'installation sous Linux et UNIX, il se peut que certains messages contextuels ne s'affichent pas clairement si vos propriétés de couleur sont blanc sur blanc.

4. Cliquez sur l'onglet Installer le produit.

5. Cliquez sur CA SDM.

6. Pour poursuivre l'installation, suivez les instructions à l'écran.

   L'Assistant de configuration s'affiche.

   Remarque : Si les hôtes Internet Protocol version 4 (IPv4) et Internet Protocol version 6 (IPv6) coexistent sur le réseau, vérifiez que les stratégies de transition, outils et mécanismes appropriés pour prendre en charge ces technologies sont installés avant de démarrer la configuration du produit. Pour de plus amples renseignements sur la configuration des serveurs, reportez-vous au Manuel d'administration.

7. Entrez et sélectionnez les renseignements nécessaires à la configuration du produit.

   Remarque : Pour de plus amples renseignements sur les champs qui s'affichent dans l'assistant, reportez-vous à l'*Aide en ligne*.

8. Suivez ensuite les instructions à l'écran pour terminer l'installation.

   CA SDM est installé sur Oracle.

9. Après avoir installé CA SDM (ou migré vers CA SDM à partir d'un système autonome CA CMDB), exécutez l'utilitaire cmdb_update_ambiguity. Utilisez la commande -h pour afficher les options obligatoires. L'option -d n'est pas requise dans un environnement Linux/Unix, puisque Oracle est la valeur par défaut.

   Remarque : Pour de plus amples renseignements sur le calcul de l'index d'ambiguïté, reportez-vous au *Manuel d'administration*.

Configuration du visualiseur

Vous pouvez configurer le visualiseur pendant l'installation de CA SDM. Quand vous cochez la case Configurer le visualiseur, les panneaux de configuration du visualiseur s'affichent.

Si vous cliquez sur le bouton Suivant de l'assistant, vous validez les informations de configuration. Après une validation réussie, la tâche de configuration du visualiseur utilise les information sur la configuration du Visualiseur qui ont été validées.

Configuration du visualiseur sur un serveur secondaire

Vous pouvez configurer le visualiseur sur un serveur CA SDM secondaire pour utiliser des services Web. Le démarrage et la configuration du visualiseur s'effectuent sur un serveur secondaire pendant la configuration de CA SDM, à l'aide de l'utilitaire *pdm_edit*.

Remarque : Lorsque vous configurez des services Web secondaires sur une installation secondaire du visualiseur CA CMDB, sélectionnez le nom du serveur dans le menu déroulant. Par défaut, le serveur principal est sélectionné.

1. Sur la page du visualiseur de l'assistant de configuration, sélectionnez Configurer le visualiseur.
2. Sélectionnez un serveur CA SDM secondaire comme hôte Web et indiquez le port de l'hôte Web.

   Si la configuration s'exécute sur un serveur CA SDM secondaire, vous pouvez utiliser le menu déroulant pour sélectionner les valeurs des propriétés general.primary_server_node et general.local_host. des hôtes du service Web disponibles.
3. Entrez le numéro de port CA SDM du serveur du visualiseur secondaire.

4. Suivez ensuite les instructions à l'écran pour terminer l'installation.

   Le visualiseur est installé et configuré sur un serveur CA SDM secondaire.

5. Ouvrez une invite de commande et accédez au dossier $NX_ROOT\samples\pdmconf. Exécutez la commande suivante :
   `pdm_perl pdm_edit.pl`

   Un menu s'affiche.

6. Sélectionnez Z pour modifier les serveurs Tomcat du visualiseur. Entrez A pour ajouter un nouveau serveur Tomcat au visualiseur.

   Vous êtes alors invité à entrer un nom d'hôte.

7. Indiquez le nom de l'hôte secondaire.

   Le nom de l'hôte secondaire est enregistré et une liste de modèles apparaît.

8. Suivez les instructions fournies par l'utilitaire pdm_edit.pl.

   La configuration de Tomcat dans le visualiseur secondaire est terminée.

Configuration des composants de l'Automatisation du soutien

CA SDM installe et configure les composants suivants de l'Automatisation du soutien :

- Client utilisateur final
- Interface d'analyste de l'Automatisation du soutien
- Serveur

Vous installez et configurez séparément les composants suivants :

- Agent utilisateur final
- IDE de l'éditeur de tâches automatisées

Important : Vous *devez* installer l'option *supportautomation_url* après avoir installé CA SDM, en plus de configurer Automatisation du soutien pendant la configuration de CA SDM. Pour de plus amples renseignements sur l'option *supportautomation_url*, reportez-vous à l'*Aide en ligne*.

Configuration des modes de serveur de l'Automatisation du soutien

Vous pouvez configurer les modes de serveur suivants pour l'Automatisation du soutien lors de l'installation :

- **Serveur principal** : si vous sélectionnez le type de configuration Serveur principal, le champ Nom d'hôte ou IP utilise par défaut la valeur Nom d'hôte local. Tous les paramètres doivent obligatoirement être définis pour le serveur principal, à l'exception de la section Port interne et du champ Lier à l'adresse IP de la section Serveur de connecteur logiciel, qui sont facultatifs.

  Remarque : Configurez le serveur principal sur le serveur CA SDM suivant en fonction du type de configuration de CA SDM :

  - Conventionnelle : serveur principal ou secondaire
  - Disponibilité avancée : serveur d'arrière-plan.

  Important : Lorsque vous définissez l'*option* supportautomation_url, cette URL doit utiliser l'URL du serveur principal Automatisation du soutien. Elle ne doit pas faire référence au serveur mandataire ni au serveur d'équilibrage de la charge. Cette option s'applique uniquement au modèle conventionnel. Dans la configuration de disponibilité avancée, l'URL peut pointer vers l'équilibreur de charge, le serveur principal, ou le serveur mandataire.

  Remarque : Si vous sélectionnez l'option Serveur principal et prévoyez également configurer un ou plusieurs serveurs mandataires de connecteur logiciel, vous *devez* définir le nom d'hôte et le port externe du serveur de connecteur logiciel sur l'hôte et le port externe du mandataire de connecteur logiciel. Pour les mandataires de connecteur logiciel multiples, définissez le serveur de connecteur logiciel sur l'hôte et le port externe du serveur d'équilibrage de la charge.

- **Serveur mandataire de connecteur logiciel** : vous pouvez sélectionner le type de configuration Serveur mandataire de connecteur logiciel sur les serveurs suivants, en fonction de la configuration de CA SDM :

  - Conventionnelle : serveur secondaire
  - Disponibilité avancée : serveur d'applications

  Les valeurs par défaut pour les champs sont affichées. Tous les paramètres de serveur mandataire de connecteur logiciel doivent être définis, sauf le champ Lier à l'adresse IP de la section Configuration du connecteur logiciel qui est facultatif.

- **Serveur de routage de messages** : vous pouvez sélectionner le type de configuration Serveur de routage de messages sur les serveurs suivants, en fonction de la configuration de CA SDM :

  - Conventionnelle : serveur secondaire
  - Disponibilité avancée : serveur d'applications

  Les valeurs par défaut pour les champs sont affichées. Tous les paramètres du serveur de routage de messages doivent être définis, sauf le champ Lier à l'adresse IP de la section Configuration de connecteur logiciel qui est facultatif.

Configuration de l'Automatisation du soutien sur un serveur secondaire

Vous pouvez configurer l'Automatisation du soutien sur un serveur CA SDM secondaire.

1. Sélectionnez l'Automatisation du soutien dans l'assistant de configuration.
2. Entrez les données appropriées à vos types de configurations sur le serveur secondaire, par exemple le nom d'hôte et le port sur un serveur de connecteur logiciel.

   Important : Une fois qu'un serveur d'Automatisation du soutien est défini comme primaire ou secondaire, ce rôle ne peut plus être modifié.
3. Suivez ensuite les instructions à l'écran pour terminer l'installation.

   L'Automatisation du soutien est installée et configurée sur un serveur CA SDM secondaire.
4. Sur le serveur principal, ouvrez une invite de commande et accédez au dossier $NX_ROOT\samples\pdmconf.
5. Exécutez la commande suivante :
   `pdm_perl pdm_edit.pl`

   Un menu s'affiche.
6. Entrez M pour modifier les serveurs Tomcat de Automatisation du soutien. Entrez A pour ajouter un serveur Tomcat pour l'Automatisation du soutien.

   Vous êtes invité à entrer un nom d'hôte et un type de serveur.
7. Renseignez le nom d'hôte secondaire et le type de serveur.

   Le nom de l'hôte secondaire est enregistré et une liste de modèles apparaît.
8. Suivez les instructions fournies par l'utilitaire pdm_edit.pl.

   La configuration de Tomcat pour l'Automatisation du soutien secondaire est terminée.

Configuration de l'Automatisation du soutien sur le serveur d'arrière-plan

Vous pouvez configurer l'Automatisation du soutien sur le serveur d'arrière-plan si vous avez sélectionné la configuration de disponibilité avancée. Pour la configuration de disponibilité avancée, configurez le serveur principal sur le serveur d'arrière-plan.

1. Sélectionnez l'Automatisation du soutien dans l'assistant de configuration.
2. Sur la page Sélectionner une configuration, sélectionnez Disponibilité avancée dans la liste déroulante Configuration du serveur. Pour de plus amples renseignements, consultez l'Aide en ligne.
3. Sur la page Paramètres généraux, sélectionnez Serveur d'arrière-plan/Serveur de secours dans la liste déroulante Type de configuration.
4. Sur la page Automatisation du soutien, sélectionnez l'option Serveur principal.
5. Entrez les détails de configuration du connecteur logiciel et de Tomcat.
6. Suivez les instructions de l'assistant.

   Vous avez configuré l'Automatisation du soutien sur le serveur d'arrière-plan.

Configuration de l'Automatisation du soutien sur le serveur d'applications

Vous pouvez configurer l'Automatisation du soutien sur le serveur d'applications si vous avez sélectionné la configuration de disponibilité avancée. Le serveur mandataire de connecteur logiciel ou le serveur de routage de messages sont les modes de serveur d'Automatisation du soutien valides pour le serveur d'applications.

1. Sélectionnez l'Automatisation du soutien dans l'assistant de configuration.
2. Sur la page Sélectionner une configuration, sélectionnez Disponibilité avancée dans la liste déroulante Configuration du serveur. Pour de plus amples renseignements, consultez l'Aide en ligne.
3. Sur la page Paramètres généraux, sélectionnez Serveur d'applications dans la liste déroulante Type de configuration.
4. Sur la page Automatisation du soutien, sélectionnez l'option Serveur de routage de messages ou Serveur mandataire de connecteur logiciel.
5. Entrez les détails de configuration du connecteur logiciel et de Tomcat.
6. Suivez les instructions de l'assistant.

   Vous avez configuré l'Automatisation du soutien sur le serveur d'applications.

Configuration des tâches automatisées

Installez et configurez l'éditeur de tâches automatisées pour gérer les tâches automatisées que les analystes d'Automatisation du soutien utilisent pour fournir un soutien aux utilisateurs finals. L'utilisateur peut lancer une tâche automatisée à partir d'un document de connaissances et de l'interface en libre-service ou un analyste exécute une tâche automatisée pendant une session d'assistance. Les tâches automatisées fournissent aux analystes des renseignements détaillés sur l'ordinateur d'un utilisateur final. Créez des tâches automatisées de libre-service qui interagissent avec l'utilisateur final et traitent leur entrée. Ces tâches peuvent modifier le système de fichiers, le registre, le logiciel d'installation de téléchargement, etc. Configurez les tâches automatisées comme suit :

1. Installez l'éditeur de tâches automatisées.

   Lancez le programme d'installation à partir de l'emplacement suivant sur le support d'installation :

   `casd.nt\SAScriptWriter`

   Remarque : Vous pouvez également copier le programme d'installation et le déployer pour les utilisateurs appropriés dans votre environnement de soutien.

   L'éditeur de tâches automatisées est installé.

2. Ouvrez l'éditeur de tâches automatisées.

   L'installation de l'éditeur de tâches automatisées crée un raccourci sur votre bureau.

3. Définissez les paramètres de connexion suivants :

   a. Cliquez sur Outils, Serveur.

      La boîte de dialogue Configuration du serveur s'affiche.

   b. Entrez votre nom d'hôte et votre port.

      Port par défaut : 8070

   c. Entrez le nom de l'utilisateur et le mot de passe d'un utilisateur avec l'accès en lecture/écriture à l'éditeur de tâches automatisées, tel qu'un analyste d'Automatisation du soutien.

   d. Cliquez sur Test.

   e. Cliquez sur OK.

4. Créez des tâches automatisées et chargez-les sur votre serveur.

   Vous pouvez charger des tâches publiques ou les affecter à des clients hébergés spécifiques et à des clients hébergés fils.

   Important : Seuls les rôles du client hébergé du fournisseur de services avec l'indicateur Mettre à jour les données publiques activé peuvent charger les tâches et les bibliothèques vers le serveur. Tout le contenu de bibliothèque de tâches et le contenu statique sont stockés en tant que données publiques.

Installation de l'Outil de conception Web

Pour personnaliser un schéma et l'interface Web, installez l'Outil de conception Web.

1. Connectez-vous au serveur sur lequel vous voulez installer l'Outil de conception Web, selon votre configuration de CA SDM :
   - Conventionnelle : serveur principal ou secondaire, ou un ordinateur distant
   - Disponibilité avancée : serveur d'arrière-plan

     Important : L'outil de conception Web peut être uniquement exécuté sur le serveur d'arrière-plan. Le programme d'installation de l'outil de conception Web permet d'effectuer l'installation sur un autre serveur, mais il empêche une exécution autonome, ou sur le serveur de secours et le serveur d'applications. Par exemple, vous avez installé l'outil de conception Web sur un serveur autre que le serveur d'arrière-plan. Le raccourci de l'outil de conception Web apparaît dans le menu Démarrer. Si vous cliquez sur le raccourci, un message d'erreur s'affiche.
2. Insérez le support d'installation dans votre lecteur.

   Important : Si votre ordinateur ne dispose pas d'un lecteur approprié pour le support d'installation, copiez le contenu du support sur l'ordinateur sur lequel vous souhaitez installer CA SDM. Puis, démarrez l'installation. Pour une installation distante sur le réseau, vous pouvez partager un lecteur ou un dossier sur le réseau, puis vous connecter par l'entremise du réseau pour démarrer l'installation.
3. Pour sélectionner votre langue dans la liste, cliquez sur Sélectionner une langue.

   Le menu Installation s'affiche.

   Remarque : Si le menu Installation ne s'affiche pas automatiquement, démarrez l'installation en double-cliquant sur le fichier setup.exe, situé à la racine du support d'installation.
4. Cliquez sur l'onglet Installer le produit.
5. Cliquez sur Outil de conception Web.
6. Sélectionnez votre langue et cliquez sur OK.
7. Suivez ensuite les instructions à l'écran pour terminer l'installation de Outil de conception Web.

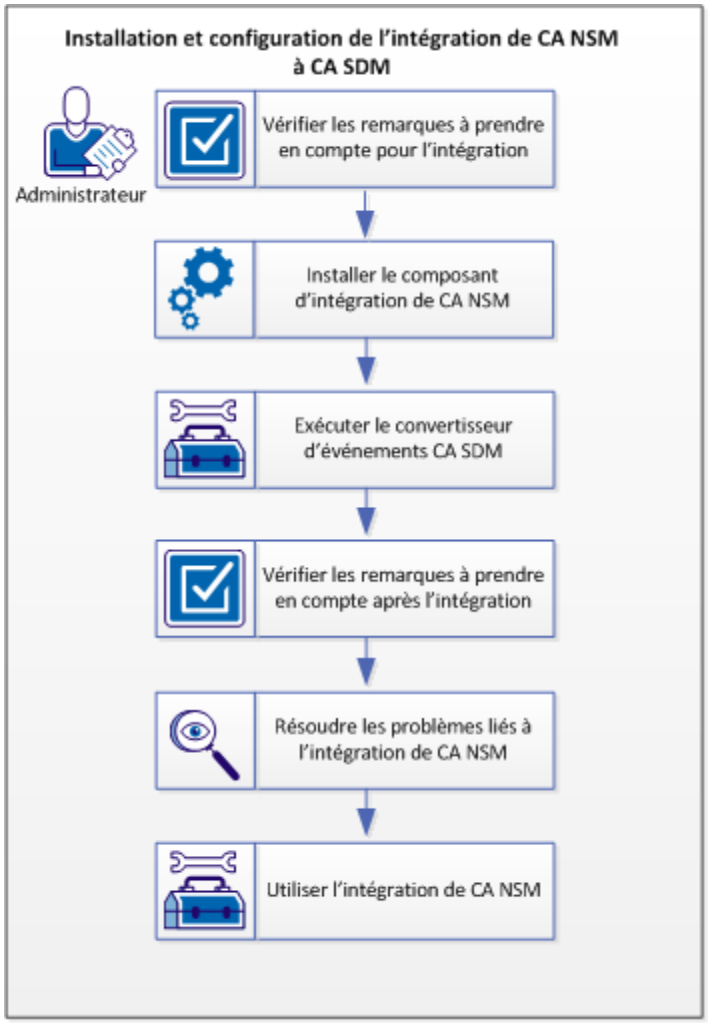
   L'Outil de conception Web est installé.

Installation et configuration de l'intégration de CA SDM et CA NSM

L'intégration de CA NSM vous permet d'effectuer les opérations suivantes :

- Contrôler automatiquement les problèmes de gestion de réseau détectés par le système de gestion des alertes et des événements CA NSM.
- Coordonner automatiquement les événements de gestion critiques détectés par CA NSM avec la fonction de gestion des incidents.
- Déterminer les impacts de vos administrateurs réseau et du personnel du centre de services.
- Éviter les demandes ou les avalanches d'incidents.
- Mettre à jour automatiquement les demandes ou les incidents.
- Mettre en oeuvre les règles commerciales en tant que bonnes pratiques pour la gestion de la prise en charge des réseaux et des services
- Distribuer automatiquement les nouvelles occurrences de requêtes ou d'incidents.
- Automatiser l'interaction avec CA SDM pour réduire la charge de travail des membres du service de soutien client en éliminant certaines tâches manuelles
- Réduire le nombre de requêtes et d'incidents ouverts par les utilisateurs en cas de problème au sein de l'entreprise, car la requête ou l'incident a été automatiquement créé dès son apparition.

Le schéma suivant illustre l'installation et la configuration de l'intégration de CA SDM et CA NSM :


Installation et configuration de l'intégration de CA NSM à CA SDM
Administrateur
Vérifier les remarques à prendre en compte pour l'intégration
Installer le composant d'intégration de CA NSM
Exécuter le convertisseur d'événements CA SDM
Vérifier les remarques à prendre en compte après l'intégration
Résoudre les problèmes liés à l'intégration de CA NSM
Utiliser l'intégration de CA NSM

1. Consultez les remarques sur l'intégration (page 180).
2. Installez le composant d'intégration de CA NSM (page 181).
3. Exécutez le convertisseur d'événements CA SDM (page 184).
4. Consultez les remarques sur la post-intégration (page 185).
5. Résolvez les problèmes d'intégration de CA NSM (page 185), au besoin.
6. Utilisez l'intégration de CA NSM (page 217).

Renseignements supplémentaires :

Création d'actifs détenus (page 186)
Surveillance des messages de la console d'événements (page 187)
Remarques relatives aux règles de filtre (page 188)
Dépannage de l'intégration de CA NSM (page 212)

Consultation des remarques sur l'intégration

Avant d'initier l'intégration, tenez compte des remarques suivantes :

- Vérifiez que vous avez installé et configuré CA SDM et CA NSM r11.2 SP2 cum1 avec le correctif WSDL.
- La modification des paramètres par défaut lors de l'intégration de CA SDM à CA NSM peut produire des résultats inattendus. Pour éviter la création instantanée de milliers de demandes CA SDM lors de l'intégration, vérifiez que les paramètres suivants dans le fichier NX.env situé dans $NX_ROOT (UNIX) ou dans le répertoire d'installation (Windows) sont définis sur Non :

  ```
  @NX_TNG_OBJECT_UPDATED_SUBSCRIBE=NO
  @NX_TNG_OBJECT_ADDED_SUBSCRIBE=NO
  @NX_TNG_OBJECT_DELETED_SUBSCRIBE=NO
  @NX_TNG_OBJECT_STATUS_UPDATED_SUBSCRIBE=NO
  ```

- Vous pouvez installer l'intégration de CA NSM sur les serveurs suivants, selon votre configuration de CA SDM :
  - Conventionnelle : serveur principal ou secondaire, ou tout autre serveur autonome
  - Disponibilité avancée : l'un des serveurs d'applications ou tout autre serveur autonome

    Important : Pour installer l'intégration de CA NSM sur un serveur autonome, installez le composant d'intégration de CA NSM (page 181) sur le serveur autonome. Pour la configuration de disponibilité avancée, pointez le composant vers l'un des serveurs d'applications.

- Si vous prévoyez d'installer CA SDM et CA NSM sur le même ordinateur, vous ne devez pas installer l'intégration de CA NSM. Cette intégration est activée automatiquement.
- (Windows) Si vous prévoyez d'installer CA SDM et CA NSM sur des ordinateurs différents, effectuez l'une des opérations suivantes, selon la configuration de CA SDM :
  - Conventionnelle : installez et configurez le serveur secondaire sur le serveur CA NSM ou installez le composant d'intégration de CA NSM (page 181) sur le serveur CA NSM.
  - Disponibilité avancée : installez et configurez l'un des serveurs d'applications sur le serveur CA NSM ou installez le composant d'intégration de CA NSM (page 181) sur le serveur CA NSM, en pointant vers l'un des serveurs d'applications.
- (UNIX) Si vous prévoyez d'installer CA SDM et CA NSM sur des ordinateurs différents, effectuez l'une des opérations suivantes, selon la configuration de CA SDM :
  - Conventionnelle : installez le serveur secondaire sur le serveur CA NSM.
  - Disponibilité avancée : installez le serveur d'applications sur le serveur CA NSM.

Installation du composant d'intégration de CA NSM

Si CA SDM et CA NSM ne sont pas installés sur le même ordinateur, ou si vous voulez installer l'intégration de CA NSM sur un serveur autonome, vous devez installer le composant d'intégration de CA NSM (ou convertisseur d'événements). Ce composant s'exécute uniquement sur un ordinateur Windows.

1. Connectez-vous au serveur de CA NSM ou au serveur autonome.
2. Insérez le support d'installation dans votre lecteur.

   Important : Si votre ordinateur ne dispose pas d'un lecteur approprié pour le support d'installation, copiez le contenu du support sur l'ordinateur sur lequel vous souhaitez installer CA SDM. Puis, démarrez l'installation. Pour une installation distante sur le réseau, vous pouvez partager un lecteur ou un dossier sur le réseau, puis vous connecter par l'entremise du réseau pour démarrer l'installation.
3. Pour sélectionner votre langue dans la liste, cliquez sur Sélectionner une langue.

   Le menu Installation s'affiche.

   Remarque : Si le menu Installation ne s'affiche pas automatiquement, démarrez l'installation en double-cliquant sur le fichier setup.exe, situé à la racine du support d'installation.
4. Cliquez sur l'onglet Installer le produit.

5. Cliquez sur CA NSM Integration.
6. Suivez les instructions à l'écran et remplissez les renseignements suivants lorsque vous y êtes invité :
   - Nom de l'hôte slump
   - Adresse IP de l'hôte slump
   - ID de port slump
   - Référentiel de NSM

   Le programme d'installation crée le fichier NX.env et un service Windows pour démarrer et arrêter le convertisseur d'événement.
7. Connectez-vous au serveur suivant, selon votre configuration de CA SDM :
   - Conventionnelle : serveur principal ou secondaire
   - Disponibilité avancée : l'un des serveurs d'applications
8. Accédez au répertoire suivant et ouvrez le fichier topology.cgf :

   `$NX_ROOT/site/eh`
9. Vérifiez que le fichier contient les renseignements suivants :

   ```
   # <remote_node>:uniconv uniconvert IP_ADDR_tngfilter:tngfilter uni

   IP_ADDR_tngcnv:tngcnv tngcnv <IP_ADDR_tngfilter>:tngfilter tng

   IP_ADDR_tngfilter:tngfilter filter_nxd <IP_ADDR_tngwriter>:tngwriter -

   IP_ADDR_tngwriter:tngwriter ehwriter - -
   ```

   IP_ADDR_tngcnv

   Désigne l'adresse IP du serveur sur lequel est exécuté le processus de conversion d'événements de CA NSM.

   IP_ADDR_tngfilter

   Désigne l'adresse IP du serveur sur lequel est exécuté CA SDM.

   IP_ADDR_tngwriter

   Désigne l'adresse IP du serveur sur lequel est exécuté CA SDM.
10. Enregistrez le fichier.

    Le composant d'intégration de CA NSM est installé.
11. (UNIX uniquement) Configurez le convertisseur d'événements (page 183).

    Le convertisseur d'événements est configuré.

(UNIX uniquement) Configuration du convertisseur d'événements

À l'issue de l'intégration de CA SDM et CA NSM, vous devez également configurer le convertisseur.

1. Connectez-vous à l'interface utilisateur Web à partir des serveurs suivants, selon votre configuration de CA SDM :
   - Conventionnelle : serveur principal ou secondaire
   - Disponibilité avancée : serveur d'applications ou d'arrière-plan
2. Sous l'onglet Administration, sélectionnez Système, Configurations.

   La page Liste des configurations s'ouvre.
3. Sélectionnez la configuration du serveur sur lequel le convertisseur d'événements est installé.

   La page Détail de la configuration s'affiche.
4. Cliquez sur Processus supplémentaires.

   La liste de processus supplémentaires s'affiche.
5. Cliquez sur Ajouter un processus.

   La fenêtre Créer un processus s'ouvre.
6. Sélectionnez Convertisseur UNI comme processus.
7. Entrez l'adresse IP du serveur sur lequel le convertisseur d'événements est installé.
8. Cliquez sur Enregistrer.
9. Exécutez pdm_configure sur le serveur suivant selon la configuration de CA SDM :
   - Conventionnelle : serveur principal
   - Disponibilité avancée : serveur d'applications
10. Les nouveaux paramètres de configuration seront appliqués au prochain démarrage du serveur.

    Important : Ne réinitialisez pas votre base de données lors de la reconfiguration.
11. En tant qu'utilisateur à forts privilèges, exécutez pdm_proctor_init sur le serveur CA NSM pour démarrer le module de surveillance de CA SDM.
12. En tant qu'utilisateur à forts privilèges, redémarrez les services CA SDM pour lancer les démons CA SDM. Exécutez pdm_status pour afficher l'état des démons.

    Le convertisseur d'événements est configuré.

Convertisseur d'événements CA SDM

Ces renseignements s'appliquent uniquement à l'intégration de CA NSM à un environnement d'exploitation Windows. Le convertisseur d'événements CA SDM s'installe selon deux méthodes différentes lorsque vous procédez à la configuration de CA SDM sur un serveur Windows :

- Installation en tant que service Windows
- Installation en tant que serveur de démons CA SDM à partir duquel vous pouvez démarrer et arrêter le convertisseur.

S'il est possible de démarrer le convertisseur sur les serveurs CA SDM à l'aide de l'une ou l'autre des deux méthodes, en fonction de votre configuration de CA SDM, vous ne pouvez en revanche le démarrer que comme service Windows sur un client.

Remarque : Si, pour une raison ou une autre, CA SDM est fermé, vous pouvez laisser le convertisseur d'événements s'exécuter, de sorte qu'il puisse toujours recevoir des messages en provenance de NSM. Tous les messages reçus de NSM pendant l'arrêt de CA SDM sont placés en file d'attente et traités lors de son redémarrage.

Suppression du convertisseur d'événements (service Windows)

Si vous souhaitez démarrer et arrêter le convertisseur d'événements par l'entremise du gestionnaire de démons, utilisez la commande suivante pour supprimer le convertisseur d'événements du service Windows :

```
tngcnv –u
```

Vous pouvez réinstaller le convertisseur d'événements en tant que service Windows à l'aide de la commande suivante :

```
tngcnv -i
```

Suppression du convertisseur d'événements (Gestionnaire de démons)

Le gestionnaire de démons ne permet pas seulement de démarrer et d'arrêter le convertisseur ; il permet également de le redémarrer en cas d'arrêt accidentel. Vous pouvez utiliser *pdm_status* pour savoir si le convertisseur est en cours d'exécution ou non et déterminer s'il s'exécute sur le serveur local ou sur un serveur distant (secondaire).

Si vous souhaitez démarrer et arrêter le convertisseur d'événements par l'entremise du gestionnaire de services Windows, supprimez le convertisseur des paramètres de démarrage du gestionnaire de démons.

Pour activer ou désactiver la ligne tngcnv, connectez-vous aux serveurs suivants, selon la configuration de CA SDM et accédez à Système, Configurations à partir de l'interface utilisateur Web de CA SDM :

- Conventionnelle : serveur principal ou secondaire
- Disponibilité avancée : serveur d'applications

Important : Cette modification est supprimée si vous réexécutez la configuration de CA SDM. Si vous voulez conserver la modification après l'exécution de la configuration, modifiez *pdm_startup.tpl*.

Consultation des remarques sur la post-intégration

Tenez compte des renseignements suivants au moment d'opérer des sélections pendant le processus d'intégration :

- Pour que le processus de réception d'un événement CA NSM et de création d'un appel dans CA SDM puisse fonctionner, vous devez au préalable installer et configurer tous les composants et vous assurer qu'ils sont actifs.
- Un événement est uniquement considéré comme perdu si le service de conversion d'événements a été arrêté. Le service de conversion d'événements place en file d'attente les événements CA NSM lorsque le système CA SDM ne fonctionne pas (ce qui signifie qu'il a été suspendu et non arrêté à partir du volet Services de Microsoft Windows). Lorsque vous redémarrez CA SDM, ce dernier traite les événements placés dans la file d'attente.
- Le service de conversion d'événements CA NSM place les événements dans la file d'attente jusqu'à ce qu'ils atteignent le nombre maximal spécifié par la variable d'environnement NX_TNGCNV_QUEUE_SIZE.
- Lorsque vous procédez à la reconstitution du référentiel CA NSM après son intégration à CA SDM, les entrées du menu CA SDM sont perdues. Pour les restaurer, vous devez relancer l'intégration sur l'ordinateur Windows sur lequel CA NSM est exécuté. Pour ce faire, exécutez le fichier integAHD.exe qui se trouve dans *répertoire-installation*\bin.
- Si le convertisseur d'événements CA NSM démarre pendant la génération d'événements CA NSM, les événements qui surviennent avant son initialisation complète seront perdus.

Vérification de CA NSM Integration

Pour vérifier l'intégration de CA NSM, effectuez les actions suivantes :

- Créez des actifs détenus. (page 186)
- Surveillez les messages de la console d'événements. (page 187)
- Remarques relatives aux règles de filtre (page 188)

Création d'actifs détenus

De nombreux produits CA Technologies créent des actifs dans la CA MDB, lesquels ne sont pas automatiquement disponibles dans CA SDM. Généralement, une organisation CA SDM souhaite uniquement suivre les actifs qu'elle possède et qui ont été acquis par un processus formel. Certains périphériques détectés par d'autres produits CA Technologies sur le réseau devraient ne pas être automatiquement disponibles dans CA SDM. Par exemple, l'ordinateur portable d'un consultant en visite n'a à priori aucun intérêt pour l'organisation CA SDM.

Pour faire en sorte qu'un actif détecté dans la CA MDB devienne disponible dans CA SDM, utilisez la boîte de dialogue de sélection des actifs détectés à partir des formulaires Rechercher un actif ou Créer un actif dans l'interface Web d'analyste.

Remarque : La boîte de dialogue de sélection Actifs détectés est disponible sur le client Web.

Si l'intégration de WorldView est utilisée, les actifs détectés peuvent être rendus disponibles dans CA SDM à partir de l'utilitaire de ligne de commande pdm_nsmimp. La carte 2D/3D et l'explorateur Unicenter CA NSM vous permettent de créer des demandes et d'y accéder à l'aide de deux options de menu accessibles en cliquant avec le bouton droit de la souris sur un objet géré : Créer une demande et Liste des demandes. Ces options de menu sont ajoutées à CA NSM lors de l'intégration à CA SDM.

Enregistrement des actifs détectés

L'utilitaire pdm_discimp est utilisé pour l'enregistrement par lots d'actifs découverts non-CA SDM. Il permet également de rechercher dans la CA MDB des composants enregistrés par d'autres produits logiciels et de les enregistrer en tant qu'actifs CA SDM afin de les exploiter dans CA SDM. Il s'agit d'un processus de traitement par lots interactif.

Le principe est similaire à celui de la boîte de dialogue Actifs découverts accessible depuis le formulaire Web de recherche/liste des actifs. Ce programme interroge les tables ca_logical_asset, ca_asset et ca_logical_asset_property à l'aide de divers paramètres et tente d'enregistrer de nouveaux actifs CA SDM à partir des valeurs découvertes.

Remarque : Si une étiquette d'actif vide est obtenue à l'issue du traitement, la valeur trouvée pour le nom d'hôte ou le nom DNS est utilisée en tant qu'étiquette de l'actif. Les composants doivent disposer au minimum d'une étiquette et d'une classe de composants pour être enregistrés et utilisés dans CA SDM.

En raison de la structure de la base de données CA MDB et de l'architecture de CA SDM, les requêtes sont soumises afin de sélectionner les enregistrements appropriés à traiter.

1. Une requête extrait les lignes issues d'une jonction entre les tables ca_logical_asset et ca_asset dans laquelle l'étiquette, le numéro de série, la balise et le nom d'hôte concordent.
2. Une autre requête est effectuée pour chacune de ces lignes dans la table ca_logical_asset_property afin de trouver des correspondances pour les champs dns_name et mac_address.

   L'actif extrait lors de la première requête est choisi pour être enregistré si la seconde requête renvoie des lignes.

Remarque : Ce processus peut affecter les performances.

Surveillance des messages de la console d'événements

L'installation de base d'CA SDM surveille automatiquement les modifications d'état des objets gérés et l'ajout de nouveaux objets gérés. Vous pouvez configurer votre environnement de manière à utiliser AHD.DLL pour surveiller les messages de la console sous Windows et envoyer des messages d'événements au serveur CA SDM.

Nous recommandons d'utiliser AHD.DLL pour envoyer des événements à CA SDM. Toutefois, d'autres méthodes sont disponibles lorsque la console d'événements s'exécute sur un système UNIX.

Event Management dans CA NSM vous permet d'identifier les événements auxquels vous souhaitez répondre et de spécifier une ou plusieurs actions à exécuter automatiquement. Lorsque vous avez défini un message et l'action associée, cette action s'effectue automatiquement chaque fois que l'événement se produit.

Après intégration à CA SDM et dès l'apparition du message d'événement, vous pouvez envoyer des données d'événements génériques à CA SDM pour :

- Créer des demandes ou mettre à jour des demandes existantes
- Créer et publier des annonces sur le tableau d'affichage CA SDM.

Remarque : Pour de plus amples renseignements sur la création de demandes et d'annonces, reportez-vous à l'*Aide en ligne*.

Pour commencer l'intégration, procédez comme ceci :

1. Utilisez AHD.DLL pour créer un enregistrement CA NSM msg_action.
2. Utilisez la commande cawto pour transférer cet enregistrement de message à la console d'événements.

Remarque : Vous devez utiliser les règles de rédacteur et de filtre par défaut fournies avec CA SDM jusqu'à ce que vous soyez certain que votre système est intégré. Ne modifiez pas et ne supprimez pas les règles par défaut tant que vous n'avez pas vérifié que les événements CA NSM créent des demandes. Évitez d'utiliser la combinaison de caractères espace, deux-points, deux-points, espace (::) lors de la création des chaînes de caractères pour les messages CA NSM. Sans quoi, une erreur d'analyse peut se produire lorsque le produit traite le message.

Envoi de données d'événements génériques (UNIX uniquement)

Pour envoyer des données d'événement génériques pour filtrer des démons dans CA SDM, utilisez le démon uniconv dans une action de message dans l'outil de gestion des événements de CA NSM.

Ces données d'événements génériques permettent ensuite de générer automatiquement des appels, de la même manière qu'avec AHD.DLL sous Windows. Il s'agit de la méthode recommandée sous UNIX.

Publication automatique d'annonces

Lorsque vous intégrez CA SDM à CA NSM, vous pouvez créer et publier des annonces sur le tableau d'affichage de CA SDM à partir de CA NSM.

Remarques relatives aux règles de filtre

Après avoir correctement configuré l'intégration et vérifié que les événements créent ou mettent à jour des demandes selon vos indications, vous pouvez modifier les règles de filtre des événements inutiles.

Voici quelques conseils pour coder les règles de filtre :

- A chaque fois que vous modifiez une règle de filtre, redémarrez CA SDM.
- Utilisez les règles de rédacteur par défaut pour tester les règles de filtre.

- Lorsque vous codez les paramètres *node_ID*, *user_ID*, ou *event_ID* dans la règle de filtre, vous devez tenir compte de la casse de l'événement entrant. Pour vérifier que la casse est correctement spécifiée, créez un événement dans CA NSM pour le paramètre que vous testez. Une demande contenant les informations dont vous avez besoin est ainsi créée. Faites correspondre la casse de la demande avec celle de la règle de filtre, Cette règle inclut la casse des messages de la console entrants.
- Evitez d'utiliser la combinaison de caractères espace, deux-points, deux-points, espace (::) lorsque de la création des chaînes de caractères pour les messages CA NSM. Sans quoi, une erreur d'analyse peut se produire lorsque le produit consomme le message.
- Lorsque vous codez une règle de filtre pour un événement donné, le texte entrant de l'événement peut être au format "Object_Status_Updated minor". Codez votre règle de filtre afin qu'elle recherche le texte ci-dessous.

  ```
  tng:::*:::*:::Object_Status_Updated.*minor.*:::(0,1)
  ```

- Les espaces dans l'événement peuvent être des caractères non imprimables. Codez le filtre afin d'inclure un ou plusieurs caractères, en utilisant un point et un astérisque (.*) à la place de l'espace (" "). Incluez également un point et un astérisque (.*) à la fin de l'événement pour les caractères non imprimables pouvant se trouver à la fin du texte.
- Lorsque vous combinez plusieurs paramètres dans un filtre, tels que *node_ID*, *user_ID* et *event_ID*, codez un filtre et vérifiez qu'il fonctionne. Ajoutez ensuite le paramètre suivant, vérifiez qu'il fonctionne en conjonction avec le premier, et ainsi de suite jusqu'à ce que tous les paramètres soient traités.
- Pour simplifier le débogage, classez vos règles de filtre de la plus spécifique (début du fichier) à la plus générale (fin du fichier).

Les règles de rédacteur d'événements suivent les mêmes pratiques de débogage que les règles de filtre. Si vous utilisez l'action CR_CREATE et que vous avez inclus un modèle, assurez-vous que ce dernier existe.

Filtrage automatique des événements

Vous pouvez configurer CA SDM afin qu'il crée automatiquement des appels pour les messages d'erreur et d'événement générés par les périphériques du réseau et d'autres sources d'événements. La définition de la méthode de filtrage vous permet de détecter automatiquement un événement et de lancer les actions spécifiées pour son traitement. Cette méthode peut améliorer l'efficacité globale du fonctionnement et réduire les risques d'erreur.

Vous pouvez configurer CA SDM pour qu'il réalise les opérations suivantes :

- filtrer les événements en fonction de l'hôte, du contenu, du type et d'autres informations provenant de CA NSM ;
- créer automatiquement des appels pour les messages d'erreur et d'événement générés par les périphériques du réseau ;
- exécuter automatiquement des commandes en réponse à un événement.

Pour filtrer automatiquement des événements, vous devez :

- définir les règles de filtre identifiant les événements qui nécessitent un traitement particulier ;
- définir les règles de rédacteur d'événements identifiant les actions à effectuer automatiquement lorsque ces événements surviennent.

Les règles de filtre et de rédacteur utilisent une structure de données d'événements génériques pour recevoir et transmettre des données. Elles sont définies à l'aide d'un éditeur de texte et sont stockées et modifiées uniquement sur le serveur CA SDM.

Tous les événements sont susceptibles d'être traités par les règles de filtre et de rédacteur. Voici quelques exemples d'événements que vous pouvez traiter de cette manière :

- Pannes matérielles
- Défaillances de processus par lots programmés
- Utilisation excessive de l'UC
- Taux de pagination élevés
- Activité de fichier inhabituelle
- Conditions de sécurité inhabituelles

Vous pouvez configurer un nombre illimité de démons de filtre, de démons de rédacteur d'événements et de sources d'événements sur des ordinateurs différents. Les emplacements de ces éléments et leurs relations sont stockés dans le fichier de topologie sur le serveur CA SDM.

Remarque : Après intégration à CA NSM, vous pouvez utiliser le démon uniconv pour générer automatiquement des demandes (méthode recommandée pour UNIX). uniconv est utilisé dans une action de message dans l'outil de gestion des événements de CA NSM.

Données d'événements génériques

Les informations sur les événements sont communiquées à l'aide d'une structure de données d'*événements génériques*. Cette structure comporte les éléments de données suivants :

Type de source

Identifie le format pour le reste de l'événement.

ID de nœud

Identifie le nom ou l'ID du périphérique.

ID d'utilisateur

Identifie le nom ou l'ID de l'utilisateur (le cas échéant).

Source majeure

Identifie l'ID de l'application source.

Source mineure

Identifie l'agent ou une autre caractéristique de l'événement.

Date/heure

Identifie la date et l'heure de l'événement.

ID d'événement

Identifie la chaîne d'événement source qui a déclenché l'événement.

Données d'événement

Identifie les données d'événement associées.

Gravité

Identifie le degré d'importance de l'événement.

Descripteur

Identifie la chaîne fournie par le démon et résultant des règles.

Source du descripteur

Identifie l'identificateur du démon ayant affecté le descripteur.

Etat du descripteur

Identifie l'état du descripteur (création, mise à jour ou fin).

Compteur d'état

Identifie le nombre de mises à jour.

Configuration des règles de filtre

Les sources d'événements envoient aux filtres des informations qui peuvent ensuite être transférées aux rédacteurs d'événements. Les périphériques du réseau générant des centaines de messages d'événements, vous pouvez utiliser des règles de filtre pour isoler ceux qui permettent de créer des appels. Les règles de filtre vous permettent d'effectuer les opérations suivantes :

- déterminer les événements ou interruptions réseau à signaler et la méthode à utiliser ;
- contrôler l'action effectuée pour chaque type d'événement ou d'interruption signalé. Les actions valides sont les suivantes : ignorer, signaler et marquer.

Lorsqu'il est intégré à CA NSM, le filtrage vous permet de gérer les événements depuis l'ensemble des systèmes gérés par CA NSM, notamment les réseaux SNA et TCP/IP.

Le filtrage des événements vous permet d'obtenir des informations spécifiques sur un nœud, une station de travail ou un utilisateur spécifique, puis de les transférer aux rédacteurs d'événements. Vous pouvez définir des règles de filtre d'événements afin de les adapter à vos propres besoins, ce qui vous permet d'identifier les événements suspects et de les corriger avant qu'ils ne posent problème.

Remarque : Il est utile de connaître les expressions régulières UNIX pour rédiger les règles de filtre. Vous pouvez également utiliser des expressions régulières UNIX sous Windows.

Définitions des règles de filtre

Les règles de filtre utilisent la mise en correspondance avec les expressions régulières UNIX pour déterminer si un événement correspond à une règle de filtre et bloquer les événements qui ne répondent pas aux critères du filtre. Un filtre spécial (ID = 5) transfère l'événement générique entrant au rédacteur sans le modifier. Le filtre transfère uniquement les événements filtrés et leur affecte une source de descripteur *filtre* et un état de descripteur *création*, *mise à jour* ou *fin*.

CA SDM utilise les champs de source majeure, d'ID d'événement, d'ID de nœud et d'ID d'utilisateur de la structure de données d'événements génériques pour rechercher une règle de filtre correspondante.

Important : les règles de filtre transfèrent les informations des événements à un autre démon qui utilise des règles de rédacteur d'événements capables de créer automatiquement des appels.

Le fichier de règles de filtre par défaut, tngfilter_rule.dat, se trouve dans le répertoire $NX_ROOT/site/eh/*IP* (UNIX) ou *répertoire-installation*\site\eh*IP* (Windows) sur le serveur CA SDM. $NX_ROOT ou *répertoire-installation* correspond au répertoire d'installation de CA SDM et *IP* désigne l'adresse IP de l'ordinateur sur lequel le filtre réside. En règle générale, cet ordinateur est le serveur CA SDM.

Ce fichier contient également de nombreuses lignes de commentaires qui vous indiquent comment définir diverses règles de filtre. Les lignes de commentaires commencent par le signe dièse (#).

Utilisez un éditeur de texte pour afficher, mettre à jour et enregistrer le fichier de règles de filtre, mais n'utilisez pas un éditeur insérant des caractères de mise en forme supplémentaires dans le fichier. Nous vous recommandons d'utiliser WordPad avec Windows et vi avec UNIX.

Syntaxe (règles de filtre)

La syntaxe des règles de filtre est la suivante :

```
source_type:::node_ID:::user_ID:::event_ID:::filter
```

où :

les champs de la règle sont séparés par trois signes deux-points (**:::**). Si vous utilisez un astérisque (*) comme caractère générique, la valeur du paramètre est ignorée lorsque le système détermine si un événement entrant répond au modèle de la règle de filtre.

Remarque : Les quatre premiers paramètres de la règle de filtre décrivent un modèle à comparer aux événements entrants. Ce modèle permet de déterminer si le filtre spécifié dans le dernier paramètre de la règle doit traiter un événement entrant.

Paramètres (règles de filtre)

source_type

Spécifie le type de source qui dirige les événements vers le filtre. Le champ de source majeure de l'événement entrant est comparé à la valeur de ce paramètre. Le type du convertisseur qui envoie les événements au filtre détermine généralement la valeur de ce paramètre. Les valeurs valides sont :

uni

Identifie le convertisseur CA NSM sous UNIX.

tng

Identifie le convertisseur CA NSM sous Windows.

Si un événement entrant correspond à plusieurs règles lors de la comparaison des types de sources et des ID d'événements, ce sont alors les ID de nœuds qui sont comparés.

node_ID

Spécifie l'ID de nœud d'origine de l'événement. Ce paramètre doit être identique à l'ID de nœud de l'événement entrant, sinon la règle de filtre ne s'applique pas. Un astérisque (*) indique que l'ID de nœud est ignoré lorsque le système détermine si un événement entrant correspond à ce modèle de règle de filtre.

Les règles qui correspondent à l' ID de noeud de l'événement entrant prévalent sur celles contenant un astérisque (*) pour ce paramètre.

Si un événement entrant correspond à plusieurs règles lors de la comparaison des types de sources, des ID d'événements et des ID de nœuds, ce sont alors les ID d'utilisateur qui sont comparés.

user_ID

Identifie un utilisateur associé à l'événement. Utilisez ce paramètre pour exécuter une action spécifique pour les événements d'un utilisateur particulier. De nombreux événements ne sont pas associés à un utilisateur particulier. Ce paramètre ne peut pas contenir d'expression régulière UNIX. Vous devez indiquer l'ID d'utilisateur exact ou un astérisque. L'astérisque (*) est la valeur par défaut et indique que l'utilisateur est ignoré lors de la sélection de la règle.

Les règles qui correspondent à l' ID d'utilisateur associé à l'événement prévalent sur celles contenant un astérisque (*) pour ce paramètre.

event_ID

Spécifie l'identificateur d'événement. Vous pouvez utiliser une expression régulière UNIX. Un point et un astérisque (.*) correspondent à tout nom d'événement. Par exemple, vous pouvez spécifier [Aa].* pour sélectionner tous les événements commençant par un "a" minuscule ou majuscule.

Si le paramètre *event_ID* se présente sous forme de texte simple (et non sous la forme d'une expression régulière), il doit être identique à l'ID de l'événement générique. La correspondance partielle n'est pas prise en compte. Si le paramètre *event_ID* est une expression régulière, la longueur de l'expression régulière correspondante permet de déterminer le degré de correspondance entre le paramètre *event_ID* de la règle de filtre et l'ID d'événement de l'événement générique.

Si un événement entrant correspond à plusieurs règles lors de la comparaison des types de sources et des ID d'événements, ce sont alors les ID de nœuds qui sont comparés.

filtre

Spécifie le filtre et les paramètres à utiliser pour traiter l'événement entrant. Le format est le suivant :

(*filter_id*, *filter_parameter1*, *filter_parameter2*, …)

Les valeurs valides pour *filter_id* sont :

Valeur=0

Consigne tous les événements.

Valeur=2

Ignore les événements peu fréquents.

Valeur=3

Ignore les interruptions dont la durée est inférieure à celle spécifiée dans *filter_parameter1*.

Valeur=4

Ignore les rafales dont la durée est inférieure à celle spécifiée dans *filter_parameter1*.

Valeur=5

Transfère tous les événements à la destination sans les modifier.

Le nombre de paramètres de filtre varie pour chaque *filter_id*, comme l'indique le tableau suivant :

filter_ID	filter_parameter1	filter_parameter2	filter_parameter3
0	0=non, 1=oui Indique si les événements doivent toujours faire l'objet de rapports distincts.	Aucun(e)	Aucun(e)
2	Nombre d'occurrences Spécifie le nombre de fois qu'un événement doit se produire dans un intervalle de temps donné pour être considéré comme significatif.	Intervalle Spécifie la durée en secondes d'un événement pour qu'il soit considéré comme significatif.	0=non, 1=oui Indique si les événements doivent toujours faire l'objet de rapports distincts.
3	Intervalle Spécifie la durée en secondes d'un événement pour qu'il soit considéré comme significatif.	0=non, 1=oui Indique si les événements doivent toujours faire l'objet de rapports distincts.	Aucun(e)

filter_ID	filter_parameter1	filter_parameter2	filter_parameter3
4	Intervalle Spécifie la durée en secondes d'un événement pour qu'il soit considéré comme significatif.	0=non, 1=oui Indique si les événements doivent toujours faire l'objet de rapports distincts.	Aucun(e)
5	Aucun(e)	Aucun(e)	Aucun(e)

Remarque : Les quatre premiers paramètres de la règle de filtre décrivent un modèle à comparer aux événements entrants. Ce modèle permet de déterminer si le filtre spécifié dans le dernier paramètre de la règle doit traiter un événement entrant.

Rédacteurs d'événements

Les rédacteurs d'événements spécifient les actions que CA SDM doit effectuer lorsqu'il détecte un événement important provenant du réseau. Ils utilisent des événements convertis (utilisant la structure de données d'événements génériques) provenant d'une source d'événements ainsi que ceux résultant d'un filtrage pour créer des appels.

Grâce aux rédacteurs d'événements, vous pouvez effectuer les opérations suivantes :

- Identifier le type d'événement provenant d'une source d'événements.
- Spécifier l'action à effectuer lorsque le rédacteur reçoit des événements de ce type. Les actions valides sont les suivantes :
  - Création de requêtes
  - Mise à jour d'appels existants
  - Exécution d'une commande
- Indiquer si la consignation est activée.

Définitions de règles du rédacteur d'événements

Lorsque vous installez CA SDM, une configuration par défaut est exécutée sur le serveur CA SDM. Elle définit une source d'événements, un filtre et un rédacteur uniques et sa règle de filtre transfère tous les événements au rédacteur. La règle de rédacteur par défaut crée des appels pour tous les événements reçus.

Le fichier de règles de rédacteur par défaut, tngwriter_rule.dat, se trouve dans le répertoire $NX_ROOT/site/eh/*IP* (UNIX) ou *répertoire-installation*\site\eh*IP* (Windows) sur le serveur CA SDM. $NX_ROOT ou *répertoire*--installation désigne le répertoire d'installation CA SDM et *IP* correspond à l'adresse IP du serveur CA SDM.

Vous pouvez afficher le contenu de ce fichier afin de consulter les définitions des règles de rédacteur par défaut et les commentaires décrivant le format des règles. Les commentaires se trouvent au début du fichier, les règles du rédacteur à la fin. Les lignes de commentaires commencent par le signe dièse (#).

Utilisez un éditeur de texte pour afficher, mettre à jour et enregistrer ce fichier, mais n'utilisez pas un éditeur insérant des caractères de mise en forme supplémentaires dans le fichier. Nous vous recommandons d'utiliser WordPad avec Windows et vi avec UNIX.

Syntaxe (règles de rédacteur d'événements)

La syntaxe de la règle de rédacteur d'événements est la suivante :

```
event_ID:::device:::user_ID:::majorSrc:::minorSrc:::action:::template:::
command:::logging:::event_token:::user_parms
```

où :

les champs de la règle sont séparés par trois signes deux-points (**:::**). Si vous utilisez un astérisque (*) comme caractère générique, la valeur du paramètre est ignorée lorsque le système détermine les correspondances pour cette règle.

Paramètres (règles de rédacteur d'événements)

event_ID

Spécifie l'identificateur auquel la règle de rédacteur d'événements s'applique. Vous pouvez utiliser une expression régulière UNIX. Un point et un astérisque (.*) correspondent à n'importe quel nom d'événement. Par exemple, vous pouvez spécifier [Aa].* pour sélectionner tous les événements commençant par un "a" minuscule ou majuscule.

Si le paramètre *event_ID* se présente sous forme de texte simple (et non sous la forme d'une expression régulière), il doit être identique à l'ID d'événement de l'événement générique. La correspondance partielle n'est pas prise en compte. Si le paramètre *event_ID* est une expression régulière, la longueur de l'expression régulière correspondante permet de déterminer le degré de correspondance entre le paramètre *event_ID* de la règle de rédacteur et l'ID d'événement de l'événement générique.

device

Indique le nom de l'objet, qui est généralement un périphérique ou un hôte associé à l'événement. Un point et un astérisque (*) sont utilisés en tant que valeur par défaut ; ils indiquent que l'objet source est ignoré lors de la sélection de la règle.

Si un événement entrant correspond à plusieurs règles lors de l'évaluation des types de sources et des ID d'événement, ce sont alors les périphériques qui sont comparés. Les règles qui correspondent au périphérique de l'événement entrant prévalent sur celles contenant un astérisque (*) pour le paramètre *device*.

Si vous avez défini des règles pour l'affectation des noms des périphériques, ce paramètre peut s'avérer utile. Par exemple, si vous nommez les périphériques se trouvant aux Etats-Unis US*xx*, vous pouvez spécifier US.* dans ce paramètre afin d'exécuter une action de rédacteur spécifique pour les événements provenant de ces périphériques.

user_ID

Identifie un utilisateur associé à l'événement. Utilisez ce paramètre pour exécuter une action spécifique pour les événements d'un utilisateur particulier. De nombreux événements ne sont pas associés à un utilisateur particulier. Ce paramètre ne peut pas contenir d'expression régulière UNIX. Vous devez indiquer l'ID d'utilisateur exact ou un astérisque. L'astérisque (*) est la valeur par défaut et indique que l'utilisateur est ignoré lors de la sélection de la règle.

Si un événement entrant correspond à plusieurs règles lors de l'évaluation des types de sources, des ID d'événement et des périphériques, ce sont alors les ID d'utilisateur qui sont comparés. Les règles qui correspondent à l'ID d'utilisateur associé à l'événement prévalent sur celles contenant un astérisque (*) pour le paramètre *user_ID*.

majorSrc

Affiche automatiquement le type de source majeur qui dirige les événements vers le rédacteur. Ce paramètre est obligatoire. Sa valeur est déterminée par la source de l'événement. Pour les événements provenant de CA NSM sous Windows, cette valeur doit être tng. Pour les événements provenant de CA NSM sous UNIX, elle doit être uni.

minorSrc

Affiche automatiquement le type de source mineur qui dirige les événements vers le rédacteur. Pour les événements provenant de CA NSM, ce paramètre contient le type d'événement. Utilisez un astérisque (*) pour accepter tous les événements.

action

Spécifie l'action qui est réalisée lorsque le rédacteur reçoit ce type d'événement, en fonction de l'une des valeurs suivantes :

CR_CREATE

Ecrit un nouvel appel pour chaque événement.

CR_UPDATE

Met à jour une ou plusieurs demandes (le cas échéant) ou en crée une si aucune appel n'a été trouvée. Par défaut, les enregistrements sont recherchés en mettant en correspondance les attributs *log_agent* et *affected_resource*. L'utilisateur peut modifier les valeurs par défaut en spécifiant une liste d'attributs d'appel.

CR_UPDATE_ONLY

Identique à CR_UPDATE, sauf qu'aucune demande n'est créée lorsque le système n'en trouve pas.

COMMAND

Exécute la commande spécifiée dans le paramètre *command*.

Remarque : Si CA SDM ne peut pas accéder à une demande ou à une demande de changement, il tente à nouveau d'effectuer la mise à jour après un intervalle de temps donné.

template

Spécifie le nom du modèle à utiliser pour créer un appel. Ce paramètre n'est pas obligatoire et est ignoré si l'action n'est pas CR_CREATE.

Remarque : Vous devez créer le modèle de demande avant de définir la règle.

commande

Spécifie la commande à exécuter si la valeur du paramètre *action* est COMMAND. Il est possible d'incorporer des arguments de substitution dans la commande, comme indiqué ci-dessous. Les arguments sont remplacés par leurs valeurs en temps réel lorsque la commande est exécutée :

&Node

Nom du périphérique ou identificateur du nœud

&User

Nom ou ID d'utilisateur

&Date

Date de l'événement

&Time

Heure de l'événement

&Event-id

Chaîne d'événement source qui a déclenché l'événement

&Data

Données d'événement associées

&Sev

Mesure de l'importance de l'événement

&Major-src

ID de l'application source

&Minor-src

Nom d'agent ou autre caractéristique de l'événement

&Handle

Chaîne fournie par le démon et qui résulte des règles

&Src-handle

Identificateur du démon ayant affecté le descripteur

&Status-handle

Etat du descripteur (les valeurs valides sont : création, mise à jour et fin)

consignation

Spécifie si une consignation se produit à l'aide de l'une des valeurs suivantes :

NONE

Aucune consignation, sauf celle des erreurs. NONE est la valeur par défaut.

PDM

La consignation est effectuée dans le journal CA SDM (stdlog.0) dans le format d'événement générique interne de ce dernier.

SYS

La consignation est effectuée dans le journal système d'UNIX qui peut ensuite être envoyé à la console d'Unicenter. Un ID de message (CAPD ....13) est affecté à l'événement afin qu'il puisse être traité depuis la console Unicenter.

BOTH

La consignation est effectuée dans le journal CA SDM (stdlog.0) et le journal système UNIX.

event_token

Il s'agit d'une balise de 30 caractères définie par l'utilisateur et utilisée pour identifier une demande spécifique associée à un attribut *event_id* (message d'événement tng) ou tous les messages semblables à un *event_id* (par exemple, attribut *event_id* avec caractères génériques). *event_token* est un attribut de demande stocké dans chaque demande générée par l'interface CA NSM. Si aucun attribut *event_token* n'est spécifié dans la règle de rédacteur, la chaîne "tng_generated" est utilisée. L'utilisateur peut ainsi mettre à jour toutes les demandes correspondant à l'attribut *event_token*. Par exemple, deux messages différents pour le même actif peuvent mettre à jour des appels uniques.

Chaque règle de rédacteur CR_UPDATE spécifie des parties de message et un attribut *event_token* uniques. L'attribut *event_token* permet de rechercher et de mettre à jour la demande correspondante. Par défaut, un journal d'activité contenant le message est ajouté à l'appel correspondant. Dans un autre exemple, l'utilisateur peut mettre à jour l'attribut d'état (par exemple, set status=CL (closed)) d'une demande existante en spécifiant le même attribut *event_token* dans la règle de rédacteur CR_UPDATE utilisée lors de la création de la demande à l'aide d'une règle CR_CREATE.

Par exemple, la première règle de rédacteur ci-dessous conduit le processus de rédacteur (tngwriter) à créer un appel avec un attribut event_token égal à "SystemCritical" lorsqu'il reçoit un événement NSM identifié par la chaîne "Event1". La deuxième règle de rédacteur force le processus de rédaction à mettre à jour la valeur de l'état sur "CL" pour toutes les demandes d'appel avec un attribut event_token égal à "SystemCritical" lorsqu'il reçoit un événement NSM identifié par la chaîne "Event2".

```
Event1:::.*:::*:::tng:::*:::CR_CREATE:::::::::NONE:::SystemCritical:::
Event2:::.*:::*:::tng:::*:::CR_UPDATE:::::::::NONE:::SystemCritical:::%SEARCH
=EVENT_TOKEN;%STATUS=CL
```

user_parms

Contient les informations suivantes :

Valeurs d'attributs d'appel

Les valeurs d'attribut de demande sont spécifiées à l'aide de la syntaxe suivante : **%***ATTRIBUT***=***valeur*, où *ATTRIBUT* est un nom d'attribut identifié dans le fichier text_api.cfg qui correspond à un attribut de demande d'appel Majic CA SDM. Ce fichier se trouve dans le répertoire $NX_ROOT/site (UNIX) ou dans *répertoire-installation*\site (Windows).

Remarque : Si vous utilisez plusieurs paires mot clé/valeur, séparez-les par un point-virgule (";").

Par exemple, la règle de rédacteur ci-dessous conduit le processus de rédacteur (tngwriter) à créer un appel avec un destinataire égale à mccda04 et un client égal à nsm lorsqu'il reçoit un événement CA NSM identifié par la chaîne Event4.

```
Event4:::.*:::*:::tng:::*:::CR_CREATE:::::::::NONE::::::%ASSIGNEE=mccda04
;CUSTOMER=nsm
```

Liste des attributs d'appel à mettre en correspondance lors de la mise à jour des enregistrements d'appel

La syntaxe de la liste des attributs à mettre en correspondance est spécifiée comme suit :

%SEARCH=attribute1[, attribute2…], où SEARCH est un mot-clé donné et attribute1, attribute2, (et ainsi de suite) sont des noms d'attributs spécifiés dans le fichier text_api.cfg.

La liste de recherche d'attributs par défaut est « asset_name » (DEVICE ou UUID) et LOG_AGENT. Le mot-clé SEARCH ajoute des attributs (pour établir une correspondance) à la liste de recherche par défaut. Le mot clé SEARCH_EXPLICIT remplace intégralement la liste de recherche par défaut. Seule la liste des attributs suivant le mot-clé SEARCH_EXPLICIT est utilisée pour rechercher un appel.

Par exemple, la règle de rédacteur ci-dessous conduit le processus de rédacteur (tngwriter) à mettre à jour la valeur de l'état sur CL pour toutes les demandes d'appel avec un destinataire correspondant à mccda04 lorsqu'il reçoit un événement CA NSM identifié par la chaîne Event2.

```
Event2:::.*:::*:::tng:::*:::CR_UPDATE:::::::::NONE:::SystemCritical:::%SE
ARCH=ASSIGNEE;%STATUS=CL;%ASSIGNEE=mccda04
```

un attribut de la liste des valeurs d'attributs est utilisé si l'attribut figure dans la liste SEARCH ou SEARCH_EXPLICIT. S'il n'y figure pas, il est alors utilisé pour définir ou mettre à jour la valeur de l'attribut dans l'appel. Il ne peut être utilisé pour les deux dans la même règle de rédacteur.

Remarque : Pour plus d'informations sur text_api.cfg et son utilisation par CA SDM, reportez-vous au *Manuel d'administration*.

Noms de paramètres spéciaux remplacés par leur valeur respective provenant de la structure d'événements CA NSM

Vous pouvez utiliser les noms de paramètres spéciaux suivants n'importe où dans la chaîne *user_parms* :

&Message

Texte associé à ce message de CA NSM.

&Parm

Champ du paramètre AHD.DLL de l'écran d'action de message de CA NSM.

&Uuid

Identificateur universel unique de CA NSM.

&Device

Périphérique (par exemple, nom d'hôte) qui a généré le message CA NSM.

&Majorsrc

Type de source majeur qui dirige les événements vers le rédacteur. Pour les événements provenant de CA NSM sous Windows, cette valeur est tng. Pour les événements provenant de CA NSM sous UNIX, cette valeur est uni.

&Minorsrc

Type de source mineur qui dirige les événements vers le rédacteur.

&Node

Périphérique (par exemple, nom d'hôte) qui a généré le message CA NSM.

&Addr

Adresse IP de l'hôte qui a généré le message CA NSM.

&Username

Nom d'utilisateur de l'hôte qui a généré le message de CA NSM.

&Date

Nombre entier indiquant le temps écoulé depuis la création du message CA NSM en 1970.

&Time

Date et heure du message CA NSM (par exemple, mar 4 juil 10:23:37 2000).

&Severity

Gravité du message CA NSM.

&Tag

Données de balise associées au message de CA NSM.

Par exemple, la règle de rédacteur ci-dessous conduit le processus de rédacteur (tngwriter) à créer un appel avec un client égal à la valeur du nom d'utilisateur (&username) du message d'événement lorsqu'il reçoit un événement NSM identifié par la chaîne "Event2".

```
Event2:::.*:::*:::tng:::*:::CR_CREATE:::::::::NONE::::::%CUSTOMER=&Username
```

Les paramètres *event_token* et *user_parms* vous permettent de définir les valeurs initiales ou de mettre à jour les valeurs de tous les attributs de la demande et de spécifier les champs à mettre en correspondance lors de la recherche des enregistrements à mettre à jour. La seule restriction est que l'attribut de description n'est jamais mis à jour dans un enregistrement d'appel existant. Si une mise à jour d'enregistrement et le champ de description sont spécifiés, un journal d'activité contenant le texte de la description est ajouté à l'enregistrement existant.

Enregistrement d'action de message CA NSM : ahd.dll AHD_Call <parms...>

Vous pouvez également spécifier des données (<parms...>) dans l'AHD_Call de l'enregistrement d'action sur message CA NSM et les utiliser pour remplacer le paramètre &Parm défini dans le paramètre user_parms de votre règle de rédacteur. Pour que les données (<parms...>) spécifiées dans l'AHD_Call soit traitées ainsi, elles doivent être précédées d'un caractère % et le paramètre spécial &Parm doit apparaître dans le champ user_parms de la règle de rédacteur.

L'exemple ci-dessous présente une action sur message CA NSM et une règle de rédacteur dont l'utilisation combinée amène le processus de rédacteur à créer des appels avec une personne assignée définie sur mccda04 lorsqu'il reçoit un événement NSM identifié par la chaîne Event3.

Ahd.dll AHD_Call %ASSIGNEE=mccda04

```
Event3:::.*:::*:::tng:::*:::CR_CREATE:::::::::NONE::::::&Parm
```

Il est possible que les clients CA SDM procédant à une mise à niveau à partir de AHD4.5 (ou version antérieure) utilisent déjà le champ <parms...>. Par exemple, vous pouvez exploiter ces données pour établir une correspondance avec des règles de rédacteur. Vous pouvez continuer d'utiliser cette méthode, sans aucune modification. Si vous souhaitez employer à la fois des paramètres « anciens » et « nouveaux », vous devez alors concaténer un caractère « % » à vos anciennes données <parms..>, suivi des nouvelles données.

Exemple :

ahd.dll AHD_Call données anciennes

ahd.dll AHD_Call %nouvelles données user_parms

ahd.dll AHD_Call données anciennes%nouvelles données user_parms

Les données insérées avant le premier caractère % sont concaténées au message d'événement CA NSM placé dans le champ de description Appel. C'est ainsi que fonctionnait CA SDM par le passé. Les données insérées après le caractère « % » sont utilisées pour remplacer le paramètre &Parm où qu'il soit spécifié dans le paramètre user_parms de votre règle de rédacteur.

Syntaxe du journal CA SDM (stdlog.0)

La syntaxe des entrées du fichier stdlog.0 est la suivante :

```
genDate genTime genNode genProc PID level codefile linenum msgID
:::msgDomain\msgNode ::: ::: :::msgGenDomain\msgGenUser:::domainID
:::msgDate msgTime:::eventID arg tag::: :::IPaddr:filter:filterNum
:::majorSrc ::: :::msgSrc:::msgType:::msgSrcNum ::: :::platform
```

où :

les champs de la règle sont séparés par trois signes deux-points (**:::**).

genDate

Spécifie le mois et le jour (à partir de l'horloge système) où l'incident de journal a été généré.

genTime

Spécifie l'heure (à partir de l'horloge système) à laquelle l'incident de journal a été généré.

genNode

Spécifie le nom du nœud ayant généré l'incident de journal. La valeur correspond généralement aux huit premiers caractères du nom DNS du noeud générant l'incident. Cette valeur est toujours la même car stdlog.0 contient uniquement des entrées de processus s'exécutant sur le même nœud.

genProc

Spécifie le nom du processus (par exemple, ehwriter) ayant généré l'incident de journal. Le nom du processus dépend de l'environnement d'exploitation mais il doit correspondre à celui qui s'affiche dans la liste des processus du gestionnaire des tâches (Windows) ou dans une sortie de commande ps (UNIX).

PID

Spécifie l'identificateur de processus numérique de la liste des processus du gestionnaire des tâches (Windows) ou d'une sortie de commande ps (UNIX). Le PID est d'une importance capitale lorsque plusieurs processus s'exécutent sous le même nom. Par exemple, plusieurs agents de base de données s'exécutent généralement simultanément sous le même nom de processus.

level

Spécifie l'estimation du programmeur concernant l'importance du message. Les valeurs possibles sont les suivantes : FATAL, EXIT, RESTART, SIGNIFICANT, SEVERE, ERROR, MINIMUM, WARNING, INFORMATION, MILESTONE, TRACE et VERBOSE.

codefile

Spécifie le nom du fichier de code source à partir duquel le message a été généré.

linenum

Spécifie le numéro de la ligne du fichier de code source à laquelle le message a été généré.

msgID

Spécifie l'ID affecté à un événement TNG.

msgDomain

Spécifie le nom du domaine d'origine du message.

msgNode

Spécifie le nom du nœud d'origine du message.

msgGenDomain

Spécifie le domaine à partir duquel l'utilisateur identifié par la valeur msgGenUser a généré le message TNG.

msgGenUser

Spécifie l'ID de l'utilisateur à l'origine du message TNG.

domainID

Spécifie l'ID du domaine à partir duquel le message TNG a été généré.

msgDate

Spécifie le mois et le jour (à partir de l'horloge système) où le message TNG a été généré.

msgTime

Spécifie l'heure (à partir de l'horloge système) à laquelle le message TNG a été généré.

eventID

Spécifie la chaîne d'événement source ou l'expression régulière de type sed ayant déclenché l'événement.

arg

Spécifie une variable entrée dans la chaîne de texte d'une action sur message. Par exemple, si le champ de texte d'une action sur message est renseigné sous la forme « ahd.dll AHD_Call help me », l'argument dans stdlog.0 se présente sous la forme « args=help me ».

tag

Spécifie les données de balise associées au message TNG.

IPaddr

Spécifie l'adresse IP de l'hôte qui a généré le message TNG.

filtre

Spécifie le nom de processus pour le fichier de règles de filtre.

filterNum

Spécifie le numéro du fichier de règles de filtre.

majorSrc

Spécifie la source majeure (ou le type de convertisseur). Il s'agit d'une chaîne identifiant l'ID de l'application source. Elle indique si les événements proviennent d'Unicenter TNG pour Windows (auquel cas la valeur est tng), d'Unicenter pour UNIX (auquel cas la valeur est uni) ou d'un démon interne (auquel cas la valeur est -).

msgScr

Spécifie la source du message. Les valeurs possibles sont les suivantes : CNV (convertisseur), FLT (filtre), NOS (pas de source) et WRT (rédacteur).

msgType

Spécifie le type de message. Les valeurs possibles sont les suivantes : CRT (création), DSC (découverte), TRM (fin) et UPD (mise à jour).

msgSrcNum

Spécifie le numéro de la source du message.

platform

Spécifie l'environnement d'exploitation à partir duquel le message a été généré. Les valeurs possibles sont les suivantes : AIX, AS400, DECOSF1, DGUX, DYNIX, HPUX, IRIX, MISERVER, MPRAS, MVS, NETWARE, SINIX, SOLARIS, SVR4MP, TANDEM, UNIXWARE, WNT (Windows) ou toute autre valeur définie par les agents UNIX.

Chargement des règles de rédacteur d'événements

Lorsque vous modifiez ou définissez des règles de rédacteur, vous pouvez charger ces règles nouvelles ou modifiées sans redémarrer le serveur CA SDM, ni aucun des processus de soutien, tels que le convertisseur CA NSM ou les démons de filtre et de rédacteur. Il vous permet également de copier les règles de rédacteur existantes dans un fichier.

Pour charger des règles de rédacteur d'événements, utilisez l'utilitaire wrtrule.

Syntaxe (chargement des règles de rédacteur d'événements)

La syntaxe pour le chargement des règles de rédacteur d'événements est la suivante :

```
wrtrule [-v] -c addr [-r rule_file] [-d dump_file]
```

Paramètres (chargement des règles de rédacteur d'événements)

-v

Spécifie le mode commentaires qui affiche des commentaires durant l'exécution de l'utilitaire.

-c addr

Nom du rédacteur d'événements tel qu'indiqué par slstat.

-r rule_file

Nom du fichier texte contenant les événements à charger.

-d dump_file

Nom du fichier dans lequel vous souhaitez copier les règles de rédacteur d'événements. Les informations suivantes sont copiées dans le fichier :

- les messages d'événements en attente ;
- les informations sur les ressources réseau en cours d'extraction ;
- les règles de rédacteur d'événements.

Remarque : Bien que les paramètres -r *rule_file* et -d *dump_file* soient facultatifs, vous devez en spécifier au moins un. Vous pouvez également spécifier les deux, auquel cas les nouvelles règles sont chargées en premier.

Remarque : Si le rédacteur d'événements traite un ou plusieurs messages CA NSM quand il reçoit une demande lui indiquant de charger de nouvelles règles de rédacteur, le chargement est différé jusqu'à ce que le rédacteur ait terminé le traitement des messages en cours. Par exemple, il se peut que le rédacteur soit en train de traiter un événement car il attend des informations sur les composants réseau. Dans ce cas, le message de chargement est différé jusqu'à ce que ces informations aient été extraites et qu'un appel CA SDM ait été créé.

Une demande de copie des règles d'événements actuelles dans un fichier est cependant immédiatement exécutée.

Gestion des événements filtrés

Les relations entre des démons de filtre et de rédacteur d'événements et des sources d'événements sur des ordinateurs différents sont gérées dans le fichier de topologie (topology.cfg) situé dans le répertoire $NX_ROOT/site/eh (UNIX) ou *répertoire-installation*\site\eh (Windows) sur le serveur CA SDM. Ce fichier vous permet de déterminer et de gérer l'ensemble du système de traitement des événements de manière centralisée. Au lieu d'aller sur plusieurs clients, vous pouvez modifier les fichiers depuis un seul emplacement et déterminer la topologie de l'ensemble du système de traitement des événements.

Remarque : Le répertoire $NX_ROOT/site/eh (UNIX) ou *répertoire-installation*\site\eh (Windows) sur le serveur CA SDM contient également des règles de filtre et de rédacteur d'événements.

Utilisez un éditeur de texte pour afficher, mettre à jour et enregistrer le fichier topology.cfg, Nous vous recommandons d'utiliser WordPad avec Windows et vi avec UNIX. N'utilisez pas d'éditeur de texte qui insère des caractères de mise en forme dans un fichier.

Le format du fichier de topologie est le suivant :

```
nom cmd [nom-dest [type-convertisseur]
```

où :

nom

Spécifie l'hôte et le nom unique du démon de traitement des événements au format *nom_hôte:nom-démon* (par exemple, ws2:uconv). Le *nom de démon* apparaît dans la commande *slstat*.

cmd

Spécifie le nom de l'exécutable dans le répertoire $NX_ROOT/bin (UNIX) ou *répertoire-installation*\bin (Windows), notamment tngcnv, uniconvert, filter_nxd ou ehwriter.

nom-dest

Spécifie le démon de réception des événements génériques (par exemple, ws2:filter1 et ws3:wrtr). Les démons de rédacteur d'événements n'ont pas de démon de destination. Tous les démons doivent également disposer d'un enregistrement dans le fichier de topologie.

type-convertisseur

Spécifie si les événements proviennent de CA NSM pour Windows (tng), de CA NSM pour UNIX (uni) ou d'un démon interne (-).

Voici un exemple de fichier de topologie :

```
# maple:uniconv    uniconvert  maple:tngfilter   uni
maple:tngcnv     tngcnv      maple:tngfilter   tng
maple:tngfilter  filter_nxd  maple:tngwriter   -
maple:tngwriter  ehwriter    -                 -
```

Exemple :

L'exemple ci-dessous explique comment une organisation a mis en oeuvre des événements filtrés dans une installation intégrée de CA SDM et CA NSM.

Pour créer automatiquement des demandes lorsqu'un état critique s'affiche sur la carte WorldView de CA NSM, l'administrateur CA SDM (Jean) doit créer une règle de filtre d'événements afin d'identifier les événements auxquels il souhaite répondre. Il doit également créer une règle de rédacteur d'événements afin de spécifier l'action à effectuer lors de la réception d'événements de ce type.

Jean décide de commencer par utiliser une règle de filtre simple. Une fois familiarisé avec le système, il utilisera un ensemble de règles plus complexe. Il décide de capturer tous les événements critiques des serveurs américains. Dans un souci de simplicité, son système applique la convention qui consiste à affecter le nom usaxxx à tous les serveurs situés aux États-Unis.

Jean modifie d'abord le fichier de règles de filtre tngfilter_rule.dat situé dans le répertoire $NX_ROOT/site/eh/IP du serveur CA SDM, où IP correspond à l'adresse IP du serveur CA SDM. Il utilise l'éditeur vi d'UNIX, mais il pourrait tout aussi bien utiliser tout autre éditeur de texte n'ajoutant pas de caractères de contrôle (il est recommandé aux utilisateurs de Windows d'utiliser WordPad pour l'édition de fichiers).

Dans le fichier tngfilter_rule.dat, le signe dièse (#) est le caractère de commentaire. Les caractères qui se trouvent après le signe dièse sont ignorés lors de la lecture des règles. La plupart des lignes du fichier tngfilter_rule.dat de Jean sont commentées, mais il remarque les lignes suivantes :

```
# Report All Events (separately)
uni:::*:::*:::.*:::(0,1)
tng:::*:::*:::.*:::(0,1)
```

Elles constituent un filtre ouvert, c'est-à-dire que le filtre transfère tous les événements au rédacteur d'événements.

Jean les modifie comme suit :

```
# Report All Events (separately)
# uni:::*:::*:::.*:::(0,1)
tng:::*:::*:::Object_Status_Updated.*Critical.*:::(0,1)
```

Jean a mis la ligne uni en commentaire car, pour l'instant, il s'intéresse uniquement aux événements CA NSM sous Windows. Il entre Object_Status_Updated.*Critical.* dans le champ event_ID de la ligne tng car il souhaite que le filtre transfère uniquement les événements Object_Status_Updated.*Critical.*. CA NSM génère des événements Object_Status_Updated.*Critical.* lorsque l'état d'un objet devient critique.

Après avoir enregistré le fichier de règles de filtre, Jean modifie le fichier de règles de rédacteur, tngwriter_rule.dat, situé dans le répertoire $NX_ROOT/site/eh/IP sur le serveur CA SDM, où IP correspond à l'adresse IP du serveur CA SDM.

Comme pour les règles de filtre, la plupart des lignes du fichier sont des commentaires. Les deux dernières lignes correspondent aux définitions des règles de rédacteur par défaut. Jean souhaite se concentrer uniquement sur les événements CA NSM sous Windows et met donc la première ligne en commentaire.

Pour mettre en forme la deuxième ligne, Jean procède comme suit :

1. Ayant déjà défini le filtre de manière à ce que seuls les événements critiques soient transférés, il laisse l'ID d'événement ouvert avec .*.
2. Il souhaite accepter uniquement les événements provenant des serveurs américains et entre donc usa.* dans le champ du périphérique.
3. Désirant accepter les événements de tous les utilisateurs, il laisse le champ d'utilisateur renseigné par l'astérisque (*).
4. Il souhaite écrire un nouvel appel pour chaque événement critique et laisse donc le champ d'action défini sur CR_CREATE.
5. Ayant déjà entré un modèle d'appel approprié dans le système, il entre son nom, CriticalTemplate, dans le champ de modèle.
6. Il ne souhaite pas d'autre consignation, le champ correspondant reste donc défini sur NONE.

Une fois ces modifications apportées, les lignes se présentent comme suit :

```
# .*:::.*:::*:::uni:::*:::CR_CREATE::::::::NONE
.*:::usa.*:::*:::tng:::*:::CR_CREATE:::CriticalTemplate::::::NONE
```

Jean enregistre le fichier de règles de rédacteur, puis redémarre le serveur CA SDM. Il est maintenant prêt à recevoir des événements et à copier des appels automatiquement.

Dépannage de l'intégration de CA NSM

Des erreurs peuvent se produire lors de l'intégration, la configuration et l'utilisation de CA NSM avec CA SDM. Il est possible d'y remédier à l'aide des renseignements ci-après :

- Messages d'erreur relatifs à la carte 2D/3D (Windows uniquement) (page 212)
- Examen de la configuration du serveur (page 213)
- Messages d'erreur concernant les filtres (page 214)
- Vérification de la connexion slump (page 216)
- Activation de la consignation (page 216)

Messages d’erreur relatifs à la carte 2D/3D (Windows uniquement)

La portion d'intégration de la carte 2D/3D et de l'explorateur Unicenter peuvent produire des erreurs CA NSM.

Echec de la création de l’objet TNGWV= x

Cause :

Cette erreur se produit généralement lorsque le script d'intégration est exécuté plusieurs fois sans que la suppression de l'intégration ait été effectuée au préalable (x représente un nombre).

Action :

Pour supprimer l'intégration, puis intégrer à nouveau CA SDM à la carte 2D/3D et à l'Explorateur Unicenter de CA NSM, procédez comme suit :

1. Sur la ligne de commande, entrez :
   `répertoire-installation\bin\deintahd.exe`
2. Ouvrez l'explorateur d'objets de CA NSM. Recherchez l’objet Méthode et cliquez dessus pour afficher la liste des méthodes.
3. Si des méthodes AHD apparaissent dans la colonne Nom, sélectionnez Supprimer dans le menu Objet pour les supprimer.
4. Cliquez sur Popup_Menu pour afficher la liste des menus.

5. Si un objet AHDManagedObject apparaît dans la colonne Nom, sélectionnez Supprimer dans le menu Objet pour le supprimer.
6. Popup_Menu étant toujours ouvert, faites défiler la liste jusqu'à ce que ManagedObjects s'affiche dans la colonne Nom.
7. Recherchez toutes les occurrences de ManagedObject dont le nom de méthode contient AHD. S'il en existe, sélectionnez Supprimer dans le menu Objet pour les supprimer.
8. Cliquez sur Jasmine_Menu_Action pour afficher une liste des méthodes de l'Explorateur Unicenter. Si des actions de menu USPSD apparaissent dans la colonne Nom, sélectionnez Supprimer dans le menu Objet pour les supprimer.
9. Cliquez sur Jasmine_Menu_Action pour afficher une liste des menus de l'Explorateur Unicenter. Si des objets de menu USPSD apparaissent dans la colonne Nom, sélectionnez Supprimer dans le menu Objet pour les supprimer.
10. Quittez l'explorateur d'objets.
11. Sur la ligne de commande, entrez :

    ```
    répertoire-installation\bin\integAHD.exe
    ```

Votre intégration dans les cartes 2D/3D et l'Explorateur Unicenter devrait maintenant fonctionner correctement. Cliquez à l'aide du bouton droit de la souris sur un objet géré à partir de la carte 2D/3D ou d'CA SDM, puis vérifiez que l'ensemble des options de menu Service Desk s'affichent.

CAE0232E - Code d'erreur 22 du référentiel

Cause :

Ce message indique que le chemin d'accès au fichier exécutable dans la méthode n'est pas correct.

Action :

Ajoutez répertoire-installation\bin à votre chemin ou modifiez le champ exe_name dans la liste des méthodes pour inclure le chemin d'accès complet à l'exécutable.

Examen de la configuration du serveur

Lorsque le serveur CA SDM est installé sur un ordinateur UNIX ou Windows et que CA NSM est installé sur un autre ordinateur Windows, le serveur CA SDM doit être en cours d'exécution. Démarrez le service de conversion d'événements NSM sur l'ordinateur CA NSM. Pour vous assurer que le convertisseur d'événements fonctionne, vérifiez les processus à l'aide du gestionnaire des tâches. Si tngcnv ne s'exécute pas après le démarrage du service de conversion d'événements, vérifiez les fichiers tngcnv.*n* ou stdlog.*n* les plus récents (situés dans *répertoire-installation*\log). Ils indiquent pourquoi le convertisseur d'événements ne s'exécute pas.

Lorsque le serveur CA SDM et le serveur CA NSM opèrent sur le même ordinateur Windows, le service CA SDM doit être en cours d'exécution. Démarrez le service de conversion d'événements NSM sur l'ordinateur CA NSM. Pour vous assurer que le convertisseur d'événements fonctionne, vérifiez les processus à l'aide du gestionnaire des tâches. Si tngcnv ne s'exécute pas après le démarrage du service CA SDM, vérifiez les points suivants :

1. A l'aide de WordPad, modifiez le fichier pdm_startup qui se trouve dans *répertoire-installation*\pdmconf. Ce fichier contient un texte similaire au texte suivant :

   ```
   [ procset MAIN_PROCSET]
   pdm_info
   sw_ver_ctl
   bpnotify_nxd
   PDMBASE
   PDMBOP
   FILTERING
   ```

   Le cas échéant, supprimez le point-virgule (;) utilisé pour mettre FILTERING en commentaire.

2. Le texte suivant devrait apparaître au début du fichier :

   ```
   [ procset FILTERING ]
   tngfilter
   tngwriter
   ehc
   ; UNICNV_REPLACE
   ; tngcnv:NT_ONLY
   ```

   Le cas échéant, supprimez le point-virgule (;) utilisé pour mettre en commentaire l'une des options ci-dessus.

3. Si vous avez modifié ce fichier, enregistrez-le, puis redémarrez le serveur CA SDM.

Si le convertisseur d'événements ne s'exécute toujours pas, vérifiez le fichier *tngcnv.n* le plus récent (dans *répertoire-installation*\log). Il indique pourquoi le convertisseur d'événements ne fonctionne pas.

Messages d'erreur concernant les filtres

Si le convertisseur d'événements (tngcnv) ne démarre pas ou s'il s'exécute mais qu'aucune demande n'est créée, vos fichiers journaux contiennent peut-être une erreur indiquant pourquoi il n'a pas pu démarrer ou consigner des événements. Voici les types de messages d'erreur possibles :

Impossible de convertir un nom d'hôte en adresse IP

Cause :

Ce message indique que des entrées d'hôte manquent sur votre ordinateur CA SDM, sur votre ordinateur CA NSM ou sur les deux.

Cette erreur peut également indiquer que le DNS ne fonctionne pas ou qu'il ne renvoie pas la bonne adresse IP.

Action :

Vérifiez le fichier %SystemRoot%/system32/drivers/etc/hosts. Votre fichier d'hôte doit contenir une entrée pour l'ordinateur CA SDM et pour l'ordinateur CA NSM. Après avoir ajouté le nom d'hôte, redémarrez le convertisseur (ou le service CA SDM). Exemple d'entrée :

```
127.0.0.1       localhost        # Retour de boucle de l'hôte local
141.202.211.11  usbegp11         # Client NSM
141.202.211.12  usbegp12 ahdhost # Hôte Service Desk
                                 # (affichage de plusieurs entrées)
```

Impossible de trouver le fichier de référentiel.

Cause :

Ce message indique que le paramètre @NX_REPOSITORY n'est pas défini dans NX.env (situé dans *répertoire-installation*) sur le client.

Action :

Modifiez le fichier NX.env, ajoutez le nom exact du référentiel, enregistrez le fichier et redémarrez le convertisseur d'événements.

La dépendance n'existe pas ou elle a été marquée pour suppression.

Cause :

Ce message s'affiche lorsqu'une dépendance (probablement MSSQL) sur le convertisseur doit être supprimée.

Action :

Exécutez regedt32 et ouvrez l'arborescence HKEY_LOCAL_MACHINE -> System-> Current Control Set -> Services -> AHD_Event_Converter. Supprimez la dépendance MSSQL (ou une autre, le cas échéant), puis redémarrez le serveur Windows.

Destination inconnue, l'événement est placé dans la file d'attente ou aucune entrée de fichier topology.cfg pour le noeud ; l'événement a été placé dans la file d'attente

Cause :

Ce message indique que vous devez corriger le fichier topology.cfg sur le serveur CA SDM.

Action :

Apportez les corrections nécessaires au fichier topology.cfg (page 209), puis redémarrez CA SDM et le convertisseur CA NSM. L'exemple de fichier topology.cfg ci-dessous s'applique à un système CA SDM installé sur un ordinateur Windows et sur un ordinateur CA NSM appelés respectivement AHD1 et TNG1 :

```
TNG1:tngcnv     tngcnv      AHD1:tngfilter   tng
AHD1:tngfilter  filter_nxd  AHD1:tngwriter   -
AHD1:tngwriter  ehwriter    -                -
```

Vérification de la connexion slump

Si le convertisseur CA NSM est en cours d'exécution et qu'aucun événement n'est encore créé, vérifiez la connexion slump à CA SDM.

Pour vérifier la connexion, procédez comme suit :

1. Utilisez la commande *slstat* à partir de la ligne de commande sur l'ordinateur CA SDM.
2. Recherchez une connexion slump vers tngcnv.

   Si vous n'en trouvez pas, le convertisseur ne communique pas avec CA SDM.
3. Redémarrez le convertisseur CA NSM, puis vérifiez de nouveau la connexion.
4. Si vous ne trouvez toujours pas la connexion, vérifiez si les fichiers tngcnv.*n* (situés dans *répertoire-installation*\log) comportent des erreurs concernant tngcnv et la connexion slump dans.

Activation de la consignation

Si la connexion slump fonctionne et que vous ne voyez toujours pas de nouveaux événements, activez la consignation et recherchez dans les fichiers l'indication qu'un événement a été traité par CA NSM. Vous pouvez créer un événement simplement en modifiant l'état d'un objet géré sur la carte 2D/3D.

Pour activer la journalisation, ouvrez le fichier NX.env qui se trouve dans $NX_ROOT (UNIX) ou *répertoire-installation* (Windows) et ajoutez la ligne suivante :

```
@NX_LOG_LEVEL_BSTRAP=VERBOSE
```

Vous pouvez alors surveiller les fichiers tngcnv.*n* (situés dans *répertoire-installation*\log) pour déterminer si les événements sont transférés vers CA SDM. Un texte similaire au texte suivant devrait s'afficher :

```
09/17  16:35:58:01    tngcnv       477  MILESTONE       convrtr.c           399
Sending 1:::dogwood:::9994011e-2f7e-11d1-a435-00c04fd478c9:::17/09/97
:::16:35:41:::Object_Status_Updated minor:::BV:141.202.211.0:Segment.1
IP:141.202.211.14 MAC:  CNT:  LOC:  DSC::::3:::tngcnv:1:::tng:::WindowsNT:
::CNV:::CRT:::1:::
```

Dans cet exemple, le message indique que l'état d'un objet géré a été mis à jour à Mineur.

Si vous constatez que des événements sont transférés vers CA SDM et qu'ils s'affichent dans le journal, vérifiez que vous utilisez bien les règles de filtre et de rédacteur par défaut. Si tel n'est pas le cas, restaurez les fichiers de filtre et de rédacteur par défaut d'origine, redémarrez le serveur, puis créez un événement.

Si vous remarquez que des événements ne sont pas transférés vers CA SDM, assurez-vous que les deux processus CA NSM chargés de transmettre les informations relatives aux événements (canotify.exe et caoprdmn.exe) sont en cours d'exécution. S'ils ne s'exécutent pas, démarrez-les conformément à la procédure décrite dans la documentation de CA NSM. S'ils s'exécutent, contactez le soutien CA NSM.

Utilisation de l'intégration de CA NSM

Les exemples suivants illustrent l'utilisation de l'intégration entre CA NSM et CA SDM :

1. Création d'enregistrements de message et d'actions de message (page 218) avec une limite de contenu
2. Création ou mise à jour d'une demande à l'aide de l'utilitaire cawto (page 219)
3. Utilisation des exemples de fichiers (page 220) pour la réalisation des tâches précédentes

Remarque : Ces exemples illustrent une approche de configuration de cette fonctionnalité par défaut et ne sauraient constituer la seule méthode permettant d'accomplir cette tâche.

Exemples d'enregistrements/actions de messages avec contenu limité

Deux enregistrements de messages (CFNEW et CFUPDATE) rédigés chacun avec une seule action de message constituent la pierre angulaire de cet exemple d'intégration entre NSM et CA SDM (des exemples de fichiers sont également inclus). Pour une intégration réussie, compacte, solide et facile à gérer, vous pouvez exploiter les éléments suivants :

- Fichier tngwriter_rule.dat
- Fonctions CR_UPDATE et CR_UPDATE_ONLY
- Liste des mots-clés text_api

Remarque : L'exemple ci-dessous décrit la création d'enregistrements et d'actions de messages avec peu de contenu. Le contenu a été transféré vers les commandes cawto illustrées dans les exemples présentés plus loin. Vous pouvez également insérer directement les paramètres et le contenu souhaités dans le champ "texte" de l'action de message, ou encore utiliser une combinaison de ces deux approches.

Exemple d'enregistrement de messages du module de gestion des événements

Lorsque vous recourez à cette intégration, vous pouvez utiliser la page Enregistrement de message - Détails pour afficher un exemple d'enregistrement de message du module de gestion des événements réagissant à un événement contenant CFNEW au début de l'événement d'alerte.

Exemple de liste d'actions de messages

Lorsque vous recourez à cette intégration, vous pouvez utiliser la liste d'actions de messages associée à l'enregistrement de message CFNEW*. Lorsque vous double-cliquez sur cet élément, des informations détaillées stockées dans l'action de message s'affichent. Quand vous continuez à utilisez cette intégration, vous pouvez afficher une vue détaillée dans laquelle apparaissent le champ Action défini sur EXTERNE et le champ Texte renseigné avec la valeur de texte d'intégration standard AHD.dll AHD_Call.

Exemple d'un enregistrement de message (configuré pour rechercher des événements commençant par CFUPDATE)

Quand vous utilisez cette intégration, vous pouvez afficher des données détaillées recueillies à partir d'un deuxième enregistrement de message configuré pour la recherche d'événements commençant par CFUPDATE. Cet enregistrement de message dispose également d'une action de message identique créée pour lui (comme illustré par l'enregistrement de message CFNEW* précédent).

Exemples de commandes cawto pour la création et la mise à jour d'appels

Pour utiliser les enregistrements de messages déjà créés, envoyez un message par l'entremise du module de gestion des événements de CA NSM en utilisant l'utilitaire/la commande « cawto » fourni avec CA NSM. L'utilitaire/la commande « cawto » vous permet de créer ou de mettre à jour un appel à l'aide des formats de commande décrits dans les exemples ci-après.

Remarque : En optant pour cette approche, vous pouvez extraire et reformater (pour conversion dans un format recherché et intégration dans CA SDM) toutes les alertes intéressantes parvenant à la console de gestion des événements.

Emettez la commande "opreload" dans la console de gestion des événements de NSM pour actualiser les enregistrements et les actions de messages d'événements NSM stockés en mémoire après avoir créé les règles d'action et de message NSM précédentes.

Exemple 1 : formats "cawto" pour la création et la mise à jour d'une nouvelle demande

Utilisez le format cawto suivant pour créer un appel :

```
CAWTO -n <nom-serveur-NSM>
CFNEW;%STRING1=KEYWORD1;%CUSTOMER=ServiceDesk;%SUMMARY=Photos
requises;%CATEGORY=Applications;%DESCRIPTION=Description: Photos requises
Justification: requise par la réglementation pour la saisie
```

Utilisez le format cawto suivant pour mettre à jour un appel :

```
CAWTO -n <nom-serveur-NSM>
CFUPDATE;%STRING1=KEYWORD1;%STATUS=Fermé;%SUMMARY=Annulé par ServiceDesk
```

Exemple 2 : autres formats "cawto" pour la création et la mise à jour d'une nouvelle demande

Utilisez le format cawto suivant pour créer un appel :

```
CAWTO -n <nom-serveur-NSM> CFNEW2;%EVENT_TOKEN=KEYWORD2;%SUMMARY=Installation
serveur approuvée;%STATUS=En cours;%CATEGORY=Matériel;%DESCRIPTION=Installer
le nouveau serveur et les rattachements de niveau V à l'emplacement du serveur
existant dans le centre de données. Installer également les câbles sur le tableau
de connexions du routeur
```

Utilisez le format cawto suivant pour mettre à jour un appel :

```
CAWTO –n <nom-serveur-NSM>
CFUPDATE2;%EVENT_TOKEN=KEYWORD2;%STATUS=Fermé;%SUMMARY=Fermé par l'équipe
serveur
```

Exemples de fichiers à utiliser lors de l'intégration

Vous pouvez utiliser les exemples de fichiers suivants lors de l'intégration de CA NSM et CA SDM :

- topology.cfg (page 220)
- tngifilter_rule.dat (page 220)
- Fichier tngwriter_rule.dat (page 220)

topology.cfg

```
# <remote_node>:uniconv  uniconvert  <IP_ADDR_tngfilter>:tngfilter   uni
<IP_ADDR_tngcnv>:tngcnv  tngcnv  <IP_ADDR_tngfilter>:tngfilter   tng
<IP_ADDR_tngfilter>:tngfilter  filter_nxd  <IP_ADDR_tngwriter>:tngwriter   -
<IP_ADDR_tngwriter>:tngwriter  ehwriter  -  -
```

où :

<IP_ADDR_tngcnv>

Désigne l'adresse IP du serveur sur lequel est exécuté le processus de conversion d'événements de CA NSM.

<IP_ADDR_tngfilter>

Désigne l'adresse IP du serveur sur lequel est exécuté CA SDM.

<IP_ADDR_tngwriter>

Désigne l'adresse IP du serveur sur lequel est exécuté CA SDM.

tngfilter_rule.dat

Utilisez la version par défaut de ce fichier, sans la modifier.

Fichier tngwriter_rule.dat

Le fichier tngwriter_rule.dat se présente comme suit :

```
# evt
id:::dev:::user:::majorSrc:::minorSrc:::action:::template:::cmd:::log:::event_tok
en:::user_parms
```

où :

event id

Chaîne ou expression régulière de type sed.

device

Chaîne, expression régulière de type sed, « * » ou valeur vide.

utilisateur

Chaîne, « * » ou valeur vide.

majorSrc

Chaîne « uni » du convertisseur UNI ou « tng » du convertisseur TNG.

minorSrc

Chaîne ou « * ».

action

Options d'action. Les options suivantes sont disponibles :

CR_CREATE

Ecrit un nouvel appel pour chaque événement.

CR_UPDATE

Met à jour un ou plusieurs appels existants (le cas échéant) ou en crée un si aucun appel n'a été trouvé. Par défaut, les appels sont localisés en mettant en correspondance les champs (composants) log_agent et affected_resource. L'utilisateur peut remplacer les valeurs par défaut en spécifiant une liste d'attributs d'appels.

CR_UPDATE_ONLY

Similaire à CR_UPDATE, sauf qu'aucun appel n'est créé lorsque le système n'en trouve pas.

COMMAND

Exécute <cmd> (identifié dans la description de cmd de ce tableau).

template

Spécifie le nom du modèle à utiliser pour créer un appel. Ce paramètre n'est pas obligatoire et est ignoré si l'action n'est pas CR_CREATE.

Remarque : Vous devez créer le modèle de demande avant de définir la règle.

cmd

Commande transmise à l'interpréteur (ignorée pour toutes les actions, à l'exception de l'action COMMAND).

consignation

Options de consignation, comme indiqué ci-dessous :

NONE

Aucune consignation (sauf consignation des erreurs).

SYS

Consigne les incidents dans le journal système UNIX (console de messages Unicenter).

PDM

Consigne les incidents dans le journal d'application ($NX_ROOT/log).

BOTH

Consigne les incidents dans le journal d'application et le journal système.

event_token

(Facultatif). Balise de 30 caractères définie par l'utilisateur et utilisée pour identifier un appel spécifique associé à un attribut event_id (message d'événement tng) ou à tous les messages semblables à un event_id (par exemple, attribut event_id avec caractères génériques).

event_token est un attribut d'appel stocké dans chaque appel que crée l'interface TNG. Si aucun attribut event_token n'est spécifié dans la règle de rédacteur, la chaîne "tng_generated" est utilisée. L'utilisateur peut alors mettre à jour tous les appels correspondant à l'attribut event_token. Par exemple, deux messages différents pour le même composant peuvent désormais mettre à jour des appels uniques. Chaque règle de rédacteur CR_UPDATE spécifie des parties de message et un attribut event_token uniques. L'attribut event_token permet de rechercher et de mettre à jour la demande correspondante. Par défaut, un journal d'activité contenant le message est ajouté à l'appel correspondant.

Dans un autre exemple, l'utilisateur peut mettre à jour l'attribut d'état (par exemple, set status=CL (clôturé)) d'une demande en spécifiant le même attribut event_token dans la règle de rédacteur CR_UPDATE utilisée lors de la création de la demande à l'aide d'une règle CR_CREATE.

user_parms

(Facultatif). Cet attribut fournit les trois types d'information suivants :

- Valeurs d'attributs d'appel
- Liste des attributs d'appel à mettre en correspondance lors de la mise à jour d'enregistrements d'appel existants
- Noms de paramètres spéciaux remplacés par leur valeur respective provenant de la structure d'événements TNG

Les valeurs d'appel et la liste des attributs sont spécifiées à l'aide de la syntaxe %<MOT-CLE>=<valeur>. Si vous utilisez plusieurs paires mots-clés/valeurs, vous devez séparer chacune d'elles par un point-virgule (« ; »).

Les valeurs des attributs d'appel sont spécifiées à l'aide de la syntaxe %<ATTRIBUTE>=<valeur> où ATTRIBUTE désigne un attribut identifié dans le fichier text_api.cfg (disponible dans le répertoire $NX_ROOT/site) et correspondant à un attribut d'appel AHD au format Majic.

La syntaxe de la liste des attributs à faire correspondre est %SEARCH=<attribut1>[,<attribut2>.], où SEARCH est un mot-clé donné et attribut1 (et ainsi de suite) sont des noms d'attributs spécifiés dans le fichier text_api.cfg.

Vous pouvez utiliser les noms de paramètres spéciaux suivants n'importe où dans la chaîne user_parms :

&Message

Texte associé à ce message de CA NSM.

&Parm

Champ du paramètre AHD.DLL dans la boîte de dialogue Action de message de CA NSM.

&Uuid

Identificateur universel unique TNG.

&Device

Périphérique (par exemple, le nom d'hôte) ayant généré le message CA NSM.

&Majorsrc

Type de source majeur qui dirige les événements vers le rédacteur. Pour les événements provenant de CA NSM sous Windows, cette valeur est tng. Pour les événements provenant de CA NSM sous UNIX, cette valeur est uni.

&Minorsrc

Type de source mineur qui dirige les événements vers le rédacteur.

&Node

Périphérique (par exemple, le nom d'hôte) ayant généré le message CA NSM.

&Addr

Adresse IP de l'hôte qui a généré le message CA NSM.

&Username

Nom d'utilisateur de l'hôte sur lequel le message de CA NSM a été généré.

&Date

Nombre entier indiquant le temps écoulé depuis la création du message CA NSM en 1970.

&Time

Date et heure du message de CA NSM (par exemple, mar 4 juil 10:23:37 2000).

&Severity

Gravité du message CA NSM.

&Tag

Données de balise associées au message de CA NSM.

En suivant les exemples présentés dans l'Exemple 2 : autres formats "cawto" pour la création et la mise à jour d'une nouvelle demande, le fichier de règles de rédacteur d'événements par défaut suivant :

```
*:::.*:::*:::uni:::*:::CR_CREATE::::::::NONE
```

comme suit :

```
CFNEW.*:::.*:::*:::tng:::*:::CR_UPDATE::::::::NONE::::::&Parm;%SEARCH_EXPLICIT=S
TRING1
CFNEW2.*:::.*:::*:::tng:::*:::CR_UPDATE::::::::NONE::::::&Parm;%SEARCH=Event_Tok
en
CFUPDATE.*:::.*:::*:::tng:::*:::CR_UPDATE_ONLY::::::::NONE::::::&Parm;%SEARCH_EX
PLICIT=STRING1
CFUPDATE2.*:::.*:::*:::tng:::*:::CR_UPDATE::::::::NONE::::::&Parm;%SEARCH=EVENT_
TOKEN;%STATUS=CL
```

Remarque : Le paramètre %SEARCH_EXPLICIT est utilisé pour garantir que, lors d'une mise à jour, le système recherche une demande correspondante en comparant le contenu du champ STRING1 avant de procéder à la mise à jour. Pour plus d'informations sur le fichier text_api.cfg et la façon dont CA SDM utilise l'API Text pour créer des demandes à partir de CA NSM, reportez-vous au *Manuel d'administration*.

Informations complémentaires :

Définitions de règles du rédacteur d'événements (page 196)

Installation de CA EEM

Remarque : Avant d'installer ce composant, vérifiez et lisez les renseignements relatifs à la planification d'une installation réussie.

CA SDM r12.9 fournit CA EEM r12 CR2 sur le support d'installation.CA EEM authentifie et autorise les utilisateurs de produits CA Technologies tels que CA Workflow et CA Service Management. L'authentification signifie qu'un ID d'utilisateur et un mot de passe, ou d'autres données, vérifient qu'un produit valide est utilisé. Autoriser signifie valider le fait qu'un utilisateur connecté peut accéder à une fonctionnalité particulière du produit.

Chaque fois qu'un utilisateur essaye de se connecter, CA EEM doit authentifier ses données ; lorsqu'elles sont authentifiées, l'accès est accordé ou refusé. Par exemple, un utilisateur doit avoir un enregistrement d'utilisateur de CA EEM pour accéder à IDE ou à l'application de la liste de travail de CA Workflow. Si vous utilisez CA Workflow dans CA SDM pour gérer vos processus commerciaux, commencez par démarrer et exécuter l'installation de CA EEM dans un environnement d'exploitation pris en charge. Ensuite, installez immédiatement CA Workflow.

Important : Si vous avez une installation CA EEM existante que vous pouvez utiliser pour authentifier les produits de CA Technologies, n'installez pas CA EEM à nouveau. A la place, installez les produits de CA Technologies et référencez votre installation CA EEM existante. Toutefois, vous avez au moins besoin de la version CA EEM r8.4 SP4 CR05 avant l'intégration à CA SDM r12.9.

Installation de CA EEM (Windows)

Vous pouvez démarrer et exécuter l'installation de CA EEM sur un environnement d'exploitation pris en charge.

Important : Si vous avez une installation CA EEM existante que vous pouvez utiliser pour authentifier les produits de CA Technologies, n'installez pas CA EEM à nouveau. A la place, installez les produits de CA Technologies et référencez votre installation CA EEM existante. Toutefois, vous avez au moins besoin de la version CA EEM r8.4 SP4 CR05 avant l'intégration à CA SDM r12.9.

Pour installer CA EEM :

1. (Facultatif) Assurez-vous d'avoir installé l'environnement d'exécution Java (JRE) 1.5 et d'avoir défini la variable JAVA_HOME.

   Remarque : Vous pouvez ignorer cette étape dans CA EEM 8.4 une version ultérieure, mais un avertissement s'affiche pour vous informer que vous ne pouvez pas intégrer CA SiteMinder et SAML.

2. Insérez le support d'installation dans votre lecteur.

   Important : Si votre ordinateur ne dispose pas d'un lecteur approprié pour le support d'installation, copiez le contenu du support sur l'ordinateur sur lequel vous souhaitez installer CA SDM. Puis, démarrez l'installation. Pour une installation distante sur le réseau, vous pouvez partager un lecteur ou un dossier sur le réseau, puis vous connecter par l'entremise du réseau pour démarrer l'installation.

3. Cliquez sur Sélectionner une langue.

   Le menu d'installation s'affiche.

   Remarque : Si le menu Installation ne s'affiche pas automatiquement, démarrez l'installation en double-cliquant sur le fichier setup.exe, situé à la racine du support d'installation.

4. Cliquez sur l'onglet Installation de produits.

5. Cliquez sur CA Embedded Entitlements Manager.
6. Suivez ensuite les instructions à l'écran pour terminer l'installation de CA EEM.

   CA EEM est installé et vous pouvez installer d'autres produits de CA Technologies.

Remarque : A partir de CA SDM r12.9, les programmes d'installation CA EEM 32 bits et 64 bits sont tous deux fournis. Sur un ordinateur Windows 32 bits, CA EEM est exécuté en tant qu'application 32 bits et sur un ordinateur 64 bits, il est exécuté en tant qu'application 64 bits.

En revanche, si CA iTechnology iGateway est exécuté en tant qu'application 32 bits sur un ordinateur Windows 64 bits, CA EEM sera également exécuté en tant qu'application 32 bits.

Informations complémentaires :

Planification de l'installation de CA EEM et CA Workflow (page 116)

Configuration du kit de développement logiciel de CA EEM en mode de conformité à la norme FIPS

Lors de la configuration du serveur CA EEM en mode de conformité de la norme FIPS (Federal Information Processing Standard) , nous vous recommandons de configurer le kit de développement logiciel pour CA EEM en mode de conformité à la norme FIPS.

1. Accédez au fichier NX_ROOT/pdmconf/eiam.config.
2. Modifiez le paramètre FIPS du kit de développement logiciel Java CA EEM sur Activé.
3. Enregistrez le fichier eiam.config.

Remarque : Par défaut, le paramètre FIPS du kit de développement logiciel C++ pour CA EEM est défini sur Activé. Pour plus d'informations sur la procédure à suivre pour configurer le kit de développement logiciel pour CA EEM en mode de conformité à la norme FIPS, consultez la documentation de CA EEM.

Installation de CA EEM (UNIX)

CA EEM pour Linux et UNIX utilise un script interpréteur qui s'extrait automatiquement et vous guide tout au long du processus d'installation. Pendant le processus d'installation, le script affiche les informations de licence et vous invite à entrer les paramètres d'installation. Après avoir entré les paramètres d'installation, l'installation commence.

Important : Si vous avez une installation CA EEM existante que vous pouvez utiliser pour authentifier les produits de CA Technologies, n'installez pas CA EEM à nouveau. A la place, installez les produits de CA Technologies et référencez votre installation CA EEM existante. Toutefois, vous avez au moins besoin de la version CA EEM r8.4 SP4 CR05 avant l'intégration à CA SDM r12.9.

Pour installer CA EEM :

1. Exécutez le script d'installation approprié sur l'ordinateur cible :
   - (Linux) /lnxsrvr.cd1/ca_tps.lnx/EEM/EEMServer.bin -i console
   - (AIX) /aixsrvr.cd1/ca_tps.aix/EEM/EEMServer.bin -i console
   - (Oracle) /solsrvr.cd1/ca_tps.sol/EEM/EEMServer.bin -i console

   Le fichier est décompressé et l'installation commence.
2. Entrez Y pour accepter les termes et conditions du contrat de licence (ou sur N pour les refuser et abandonner l'installation).

   Le script vous invite à entrer les paramètres d'installation.
3. Entrez le chemin d'installation d'CA EEM (ou acceptez la valeur par défaut).

   Un écran de confirmation s'affiche avec les valeurs des paramètres d'installation que vous avez entrées.
4. Si les informations sur l'écran de confirmation sont correctes, tapez o pour poursuivre l'installation. (Si vous tapez n, vous quittez le programme d'installation.)
5. Entrez le mot de passe EiamAdmin.

   Remarque : Le nom d'utilisateur par défaut de l'administrateur est EiamAdmin.

   Le déroulement de la procédure d'installation est tributaire des paramètres de la ligne de commande et du type de trousse CA EEM installé.

   Le script du programme d'installation termine l'installation de CA EEM sur votre ordinateur.

Installation de CA Workflow

Remarque : Avant d'installer ce composant, vérifiez et lisez les renseignements relatifs à la planification d'une installation réussie.

Important : CA Workflow n'est pas inclus dans le support d'installation de CA SDM r12.9. Si vous voulez utiliser CA Workflow, téléchargez d'abord CA SDM r12.7 ISO à partir du Service de soutien de CA, puis installez CA Workflow.

Chaque fois qu'un utilisateur essaye de se connecter à CA Workflow, CA EEM authentifie ses données ; lorsqu'elles sont authentifiées, l'accès est accordé ou refusé. L'utilisateur doit avoir un enregistrement d'utilisateur de CA EEM pour accéder à l'IDE ou à la liste de travail de CA Workflow.

Après avoir installé CA EEM, démarrez et exécutez l'installation de CA Workflow sur le serveur CA SDM pour gérer vos processus commerciaux.

Important : Si vous installez CA Workflow et que vous désinstallez CA SDM, CA Workflow sera aussi désinstallé.

Les journaux de CA Workflow (*pdm_install_wf.log* et *pdm_tomcat_CAWF.log*) sont situés dans $NX_ROOT/log. Si l'installation de CA Workflow réussit, *$NX_ROOT/site/Workflow/log* contient *wf_admin.log*, *wf_process.log*, *wf_security.log* et *wl_debug.log*.

Installation de CA Workflow (Windows)

Utilisez CA Workflow pour gérer vos processus commerciaux dans CA SDM.

1. Connectez-vous au serveur CA SDM suivant, selon votre configuration de CA SDM :
   - Conventionnelle : serveur principal ou secondaire
   - Disponibilité avancée : l'un des serveurs d'applications
2. Du Service de soutien de CA, téléchargez r12.7 ISO avant de l'extraire.
3. Pour sélectionner votre langue dans la liste, cliquez sur Sélectionner une langue.

   Le menu Installation s'affiche.

   Remarque : Si le menu Installation ne s'affiche pas automatiquement, démarrez l'installation en double-cliquant sur le fichier setup.exe, situé à la racine du support d'installation.
4. Cliquez sur l'onglet Installer le produit, puis sur CA Workflow.
5. Suivez ensuite les instructions à l'écran pour terminer l'installation de CA Workflow.

   CA Workflow est installé et vous pouvez le configurer pour être utilisé avec CA SDM.

Installation de CA Workflow (UNIX)

Utilisez CA Workflow pour gérer vos processus commerciaux dans CA SDM.

1. Connectez-vous au serveur CA SDM suivant, selon votre configuration de CA SDM :
   - Conventionnelle : serveur principal ou secondaire
   - Disponibilité avancée : tout serveur d'applications
2. Du Service de soutien de CA, téléchargez r12.7 ISO avant de l'extraire.
3. Accédez au répertoire racine du fichier ISO extrait et exécutez la commande suivante pour démarrer l'installation :

   ```
   sh ./setup.sh
   ```
4. Pour sélectionner votre langue dans la liste, cliquez sur Sélectionner une langue.

   Le menu Installation s'affiche.
5. Cliquez sur l'onglet Installer le produit, puis sur CA Workflow.
6. Suivez ensuite les instructions à l'écran pour terminer l'installation de CA Workflow.

   CA Workflow est installé et vous pouvez le configurer pour être utilisé avec CA SDM.

Installation de l'IDE CA Workflow autonome

Vous pouvez installer le client autonome IDE de CA Workflow à partir du support d'installation de CA SDM sur Windows ou Linux. Pour des installations UNIX, ce client autorise les connexions au serveur UNIX de CA Workflow. Vous pouvez pointer vers l'installation de serveur CA Workflow de votre choix, quel que soit l'environnement d'exploitation, en modifiant l'URL de son IU de connexion.

CA SDM n'est pas requis pour installer l'IDE de CA Workflow. L'emplacement du journal d'installation diffère selon que le système soit doté ou non de CA SDM.

- Si CA SDM est installé sous Windows ou Linux, le journal se trouve à l'emplacement suivant :
  `$NX_ROOT/logs`
- Si CA SDM n'est pas installé, le journal se trouve dans les dossiers temporaires suivants :

  Windows

  %temp%

  Linux

  /tmp

1. Ouvrez le support d'installation de CA SDM r12.7 et choisissez l'IDE de CA Workflow.

   L'assistant d'installation des composants de CA SDM s'affiche.

2. Spécifiez l'emplacement d'installation du client de flux de travaux et cliquez sur Suivant.

   L'installation est terminée.

Journal d'installation de CA Workflow IDE

Vous *devez* vérifier que l'installation de CA Workflow IDE s'est terminée avec succès.

Pour vérifier l'installation de CA Workflow IDE

1. Accédez au répertoire spécifié dans le champ Emplacement d'installation du client de flux de travaux de l'assistant du programme d'installation du composant CA SDM.
2. Vérifiez que le répertoire contient ce qui suit :
   - Les dossiers nommés "Client" et "uninstall"
   - Les fichiers nommés *version.txt* et *wekinstall.log*

Remarque : Si l'installation présente des erreurs ou si les dossiers et fichiers se trouvent à des emplacements incorrects, consultez le fichier pdm_install_wf_client.log.

Sous Windows, vous pouvez lancer l'IDE CA Workflow à partir du menu Démarrer en sélectionnant Programmes, CA, CA Service Desk Manager, IDE CA Workflow.

Désinstallation du client CA Workflow IDE (Windows et Linux)

1. Exécutez la commande suivante :

   ```
   <install_location>/jre/bin/java" -cp
   "<install_location>/uninstall/uninstall.jar" run -silent
   ```

   install_location

   Spécifiez le dossier racine où a été installé le client IDE CA Workflow.

   - **Exemple pour Windows**

     Si "c:\test" est le dossier racine où a été installé le client IDE CA Workflow :
     `"c:\test\jre\bin\java" -cp "c:\test\uninstall\uninstall.jar" run -silent`

   - **Exemple pour Linux**

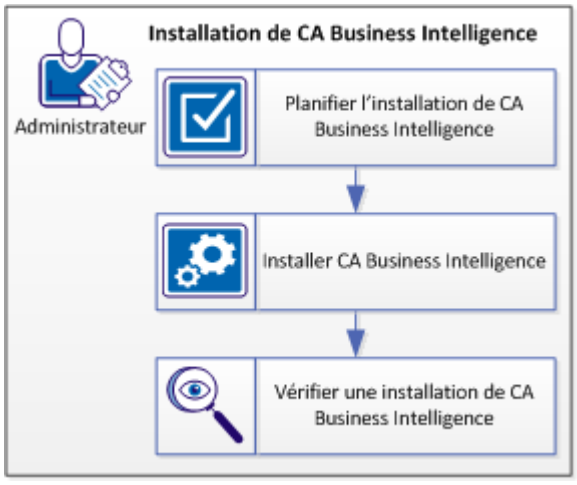
     Si "/test" est le dossier racine où a été installé le client IDE CA Workflow :
     `"/test/jre/bin/java" -cp "/test/uninstall/uninstall.jar" run -silent`

2. Supprimez le dossier racine où le client CA Workflow IDE a été installé.
3. (Windows) Supprimez le raccourci du menu Démarrer associé.

Installation de CA Business Intelligence pour CA SDM

CA Business Intelligence CA Business Intelligence fournit une installation cohérente de SAP Business Objects Enterprise Edition. Plusieurs produits CA peuvent partager une licence de CA Business Intelligence. Vous pouvez installer CA Business Intelligence dans le cadre de l'installation de CA SDM.

Le schéma suivant présente l'installation de CA Business Intelligence :


Installation de CA Business Intelligence
Administrateur
Planifier l'installation de CA Business Intelligence
Installer CA Business Intelligence
Vérifier une installation de CA Business Intelligence

1. Planifiez l'installation de CA Business Intelligence. (page 232)
2. Installez CA Business Intelligence. (page 233)
3. Vérifiez l'installation de CA Business Intelligence. (page 234)

Planification de l'installation de CA Business Intelligence

Avant de planifier la mise en oeuvre de CA Business Intelligence pour CA SDM, prenez connaissance des remarques suivantes :

- Comprenez les exigences et les remarques sur l'installation de CA Business Intelligence. Pour de plus amples renseignements, lisez les *Notes de parution* et le *Manuel de mise en oeuvre de CA Business Intelligence.*
- Désactivez temporairement tout logiciel antivirus sur l'ordinateur sur lequel vous installez CA Business Intelligence.
- L'intégration de CA SDM dans CABI prend uniquement en charge Apache Tomcat en tant que serveur d'applications CABI.
- Déterminez l'emplacement des composants à installer. Ces composants incluent le sous-réseau, l'ordinateur, la base de données, les systèmes de sécurité ou grappes spécifiques, requis pour l'exécution du système.
- Vérifiez la configuration suivante requise pour l'installation :
  - Les détails du serveur de base de données et les détails d'authentification sont disponibles.
  - Vous disposez de l'autorisation d'installation d'une nouvelle base de données SQL Anywhere ou d'utilisation d'une base de données SQL Anywhere existante.
  - Vous disposez du nom du Server Intelligence Agent (SIA).
  - Le serveur d'applications Web a été installé et configuré.
  - La liste de contrôle de l'installation du système d'exploitation sélectionné.

    Remarque : L'installation de CABI est limitée aux plates-formes Windows. Cependant, vous pouvez intégrer CABI à CA SDM sur tous les systèmes d'exploitation pris en charge.

Installation de CA Business Intelligence

Vous pouvez installer CA Business Intelligence r3.3 sur un serveur autonome en mode exprès ou personnalisé.

Remarque : Pour la configuration de disponibilité avancée, CA Business Intelligence doit être installé sur un serveur distinct.

Installation rapide

Utilisez l'installation expresse pour installer CA Business Intelligence avec tous les composants requis et facultatifs.

1. Insérez le support d'installation DVD 2 dans votre lecteur.

   Le menu Installation s'affiche.

2. Sélectionnez votre langue dans la liste Sélectionner une langue.

   Le menu Installation s'affiche.

3. Cliquez sur l'onglet Installer le produit.
4. Cliquez sur Installation de CA Business Intelligence.
5. Suivez ensuite les instructions à l'écran pour terminer l'installation de CA Business Intelligence.

   Remarque : Pour de plus amples renseignements, reportez-vous au *Manuel de mise en oeuvre de CA Business Intelligence*.

6. Redémarrez votre ordinateur lorsque vous y êtes invité.
7. CA Business Intelligence prend en charge la gamme complète d'applications de gestion des performances, de signalement, de requêtes et d'analyse. Vous devez installer CA Business Intelligence R3.3 SP1 (CABI 3.3 SP1 est une version avec correctif correspondant à la version SAP BOXI 3.1 SP6 avec correctif) pour terminer l'installation de CA Business Intelligence. Pour télécharger et installer le correctif, ouvrez le lien suivant :

   `ftp://ftp.www.ca.com/pub/CABI/CABI-3.x/boeXIR3_SP6/Windows/`

   Remarque : Pour de plus amples renseignements sur l'installation du correctif, reportez-vous aux *Notes de parution de CABI 3.3 SP1*.

8. Mettrez le correctif CA Business Intelligence R3.3 SP1 à niveau afin qu'il prenne JDK7 en charge. Pour de plus amples renseignements, reportez-vous au document *Mise à niveau de CABI 3.3 SP1 JDK à 7.pdf* disponible dans le dossier cabi-windows-boeXIR3_SP6\Docs.
9. Installez le correctif cabi33sp1hotfix patch à partir de l'emplacement suivant :

   `ftp://ftp.www.ca.com/pub/CABI/CABI-3.x/boeXIR3_SP6/Windows/`

Remarque : Utilisez le fichier readme.txt pour obtenir des instructions sur la façon d'installer le correctif.

Vous avez installé CA Business Intelligence.

Installation personnalisée

Pour installer les composants sélectionnés de CA Business Intelligence, vous pouvez utiliser l'option d'installation personnalisée. Il est conseillé d'utiliser cette option uniquement lorsque vous êtes familiarisé avec les composants SAP BusinessObjects Enterprise spécifiques et les rôles. L'installation personnalisée varie selon le choix du système d'exploitation et des bases de données. (Pour de plus amples renseignements, reportez-vous au *Manuel de mise en oeuvre de CA Business Intelligence*.)

Vérification de l'installation de CA Business Intelligence

Vérifiez l'installation correcte de CABI sur le serveur CABI afin de vous assurer qu'il s'est installé de façon appropriée.

1. Sélectionnez Démarrer, Programmes, BusinessObjects, BusinessObjects Enterprise, BusinessObjects Enterprise Java Infoview.
2. Connectez-vous à Infoview en indiquant le mot de passe de l'administrateur. Si vous pouvez vous connecter, cela signifie que CABI est installé correctement.

Vérification de l'installation

Après avoir installé CA SDM, utilisez les informations suivantes pour vérifier que l'installation a réussi.

1. Vérifiez qu'une variable d'environnement système pour le chemin d'accès est définie pour le produit dans le répertoire d'installation que vous avez spécifié. Le répertoire de base par défaut est C:\Program Files\CA\Service Desk Manager.
2. Procédez aux vérifications suivantes :
   a. Dans le panneau de configuration (Ajout ou suppression de programmes), vérifiez qu'une entrée apparaît pour le produit.
   b. Dans le menu Démarrer, vérifiez que les options suivantes s'affichent :
      - Affichez la documentation
      - Lancez l'assistant de configuration.
      - Démarrez l'interface Web
      - Contactez le soutien technique.
      - Démarrez l'Outil de conception Web.
      - Désinstallez CA SDM
3. Vérifiez que vous pouvez démarrer l'interface Web.

Important : Si vous ne pouvez pas le vérifier, le produit n'a pas été installé correctement. Dans ce cas, relancez l'installation de CA SDM pour modifier l'installation.

Informations complémentaires :

Démarrage de l'interface Web (page 246)

Fichier journal d'installation

Quand vous installez CA SDM, un fichier journal d'installation est créé pour documenter et répertorier les actions, les événements et les modifications système qui se sont produits pendant l'installation. Si le produit ne s'installe pas correctement, vous pouvez consulter les erreurs dans le fichier journal pour aider à résoudre les problèmes afin que le produit s'installe correctement.

Le fichier *ServiceDesk_r12_7_Install.log* se trouve dans le dossier \log du répertoire d'installation. Pour les installations de composants distants, le journal se trouve dans le répertoire %TEMP%. Ouvrez le fichier grâce à un éditeur de texte tel que Bloc-Notes ou l'éditeur vi.

Remarque : Si vous annulez l'installation avant qu'elle soit terminée, le journal d'installation est créé sur votre bureau (Windows) ou dans le répertoire racine (UNIX et Linux).

Chapitre 5: Configuration

Ce chapitre traite des sujets suivants :

Configuration du produit (page 237)
Configuration des composants de CA SDM (page 238)
Configuration de l'interface Web (page 241)
Mise en oeuvre de CA Business Intelligence pour CA SDM (page 247)
Configuration de l'authentification Windows intégrée pour CA SDM (page 268)
Exécution des politiques d'automatisation (page 272)
Exécution de la fiche de rapport des connaissances. (page 273)
Importation d'exemples de données Gestion des connaissances (page 274)
Configuration du moteur de recherche (page 275)
Configuration de CA Workflow (page 277)
Configuration de l'intégration des flux de travaux CA Process Automation (page 293)
Configuration de la connexion automatique (Authentification de CA MDB) (page 301)
Configurer un point d'entrée unique (page 302)
Mise en oeuvre de l'hébergement multiclient (page 303)
Procédure d'activation du basculement automatique (page 342)

Configuration du produit

Après avoir installé CA SDM et tout produit supplémentaire que vous sélectionnez, vous devez effectuer des étapes de configuration pour que les produits fonctionnent correctement ensemble. Pour configurer le produit, effectuez les opérations suivantes :

- Configurez les composants de CA SDM (serveurs, base de données, interface Web).
- Configurez l'interface Web quand le serveur Web et le serveur principal se trouvent sur des ordinateurs différents.
- Configurez l'Automatisation du soutien.
- Mettez en oeuvre les rapports de cycle de vie des documents de connaissances pour les politiques d'automatisation.
- Configurez CA Business Intelligence.
- Configurez CA Workflow.
- Mettez en oeuvre l'hébergement multiclient.

Remarque : Pour configurer des serveurs pour la configuration de disponibilité avancée, reportez-vous au scénario Configuration des serveurs pour la disponibilité avancée.

Configuration des composants de CA SDM

Si vous ne configurez pas CA SDM pendant l'installation, ou si vous configurez manuellement le produit après l'installation, vous pouvez utiliser le produit pour configurer les serveurs principal et secondaires, la base de données, l'interface Web, et les options de configuration supplémentaires.

Pour vérifier que vous pouvez correctement configurer le produit et les composants sur SQL Server, activez TCP/IP sur l'ordinateur sur lequel vous voulez effectuer l'installation et la configuration.

Important : CA SDM r12.9 ne fournit *pas* les fichiers tools.jar et javac pour AIX. Vous *devez* installer tools.jar sur AIX avant de configurer le produit. Le fichier tools.jar est requis pour pouvoir configurer les services Web REST et d'Automatisation du soutien. Pour utiliser les exemples de fichier REST, vous devez installer javac sur AIX. Vous pouvez télécharger le kit de développement logiciel Java pour AIX à partir du site Web d'IBM, dans la section IBM Developer kits pour Linux. Téléchargez les fichiers binaires 32 bits de Java SE et installez le JDK 1.6 SR10 sur l'ordinateur AIX à l'emplacement de votre choix. Copiez le fichier tools.jar à partir de l'emplacement du JDK installé dans <composant_partagé>\JRE\1.6.0_10\lib et copiez le fichier javac dans \JRE\1.6.0_10\bin. Vous pouvez également trouver l'emplacement du JRE dans la variable NX_JRE_INSTALL_DIR.

Remarque : Si les hôtes Internet Protocol version 4 (IPv4) et Internet Protocol version 6 (IPv6) coexistent sur le réseau, vérifiez que les stratégies de transition, outils et mécanismes appropriés pour prendre en charge ces technologies sont installés avant de démarrer la configuration du serveur. Pour de plus amples renseignements sur la configuration des serveurs, reportez-vous au *Manuel d'administration*.

Pour configurer les composants du produit

1. Sélectionnez Démarrer, Programmes, CA, CA Service Desk, Configuration.

   L'Assistant de configuration s'affiche.

2. Entrez et sélectionnez les renseignements nécessaires à la configuration du produit.

   Remarque : Pour de plus amples renseignements sur les champs qui s'affichent dans l'assistant, reportez-vous à *l'Aide en ligne relative à la configuration du serveur*.

3. Continuez de suivre les instructions à l'écran pour terminer l'installation du produit.

Lors de la première exécution du programme de configuration, une valeur par défaut valide pour le numéro du service TCP de la plupart des installations s'affiche. Pour déterminer le TCP Service Number (Numéro du service TCP) de votre installation, ouvrez une session telnet à partir de votre station de travail Windows sur le serveur :

- Si votre réseau utilise NIS, entrez :
  `ypcat services | grep slump.`

  Vous obtenez une ligne du type :
  `slump nnnn/tcp #Requis pour le bon fonctionnement de slump !`
- Si votre réseau n'utilise pas NIS, entrez :
  `grep slump /etc/services.`

  Vous obtenez une ligne du type :
  `#slump nnnn/tcp`

  Entrez le numéro *nnnn* dans le champ Numéro du service TCP.

Remarque : Si la configuration échoue lors de l'étape de validation des tables d'extension, la connectivité de la base de données peut poser problème. Exécutez à nouveau la configuration et vérifiez que vous avez fourni les informations de connectivité de la base de données appropriées. Pour configurer des serveurs pour la configuration de disponibilité avancée, reportez-vous au scénario Configuration des serveurs pour la disponibilité avancée.

Configuration du journal de vérification de CA CMDB

Les définitions d'objet et de déclencheur, les attributs et les formulaires HTML que CA CMDB utilise pour le journal de vérification ne sont plus les mêmes dans ce produit.

Pour configurer le journal de vérification de CA CMDB r12.9

1. Supprimez le déclencheur *cmdb_write_audit_log_site* si vous avez créé site/mods/*extension*.mod (*extension* correspond au nom d'extension).

   Dans cette version du produit, la vérification est automatiquement créée et activée.
2. Ajoutez UI_INFO(AUDIT_LOG) à chaque attribut que vous voulez consigner.
3. Utilisez les nouveaux modèles fournis par le produit pour procéder à la migration de vos formulaires HTML existants.

Remarque : Pour plus d'informations sur les attributs et les formulaires HTML, reportez-vous au *Manuel d'administration*.

Intégration de CA Cohesion ACM avec CA CMDB

Vous pouvez intégrer CA Cohesion ACM à CA CMDB à l'aide d'un correctif. Contactez le soutien CA pour obtenir le correctif adapté à votre version de CA CMDB et de CA Cohesion ACM.

Configuration du visualiseur CA CMDB pour AIX

Valide sur IBM AIX

Par défaut, CA SDM installe le visualiseur CMDB sur tous les environnements d'exploitation. Vous pouvez configurer le visualiseur CA CMDB. IBM AIX requiert des fichiers de politique de sécurité supplémentaires.

Pour configurer le visualiseur CMDB sur IBM AIX

1. Assurez-vous que le visualiseur CMDB est configuré.
2. Téléchargez les fichiers de politique illimités (version 1.4.2 ou supérieure) depuis la page des fichiers de politiques Unrestricted JCE sur le site Web d'IBM.

   Remarque : Vous devez vous inscrire sur le site Web d'IBM pour pouvoir télécharger les fichiers de politiques.
3. Remplacez les fichiers local_policy.jar et US_export_policy.jar du répertoire Shared Components JRE (emplacement par défaut : /opt/CA/SC/JRE/1.6.0_10/lib/security) par les fichiers de politiques que vous avez téléchargés a partir du site Web d'IBM.
4. Arrêtez et démarrez le visualiseur à l'aide des commandes suivantes :

   ```
   pdm_tomcat_nxd -c STOP -t VIZ
   pdm_tomcat_nxd -c START -t VIZ
   ```

   Le visualiseur CMDB est configuré pour IBM AIX.

Modification des scripts tiers pour la compatibilité de CA CMDB

Dans le cas de scripts figurant dans la version actuelle du produit, l'attribut ext_asset est renommé ID. Pour assurer la compatibilité avec d'autres produits CA Technologies utilisant l'attribut ID, vous pouvez modifier les scripts tiers qui utilisent les services Web de CA SDM pour mettre à jour les tables d'extension CA CMDB.

Pour modifier des scripts tiers pour CA CMDB

1. Ouvrez le script tiers que vous voulez modifier.
2. Remplacez toutes les références SQL de ext_asset par ID.

   Le script est compatible avec le numéro de version actuelle du produit.

Permutation du serveur cible pour les rapports de CA CMDB

En général, un système CA Cohesion ACM exporte des données de CI vers un serveur CA CMDB unique pour créer des rapports CA CMDB. Vous pouvez changer de serveur CA CMDB cible pour l'exportation des données de CI en procédant comme suit :

1. Utilisez un serveur CA CMDB en tant que cible pour exporter des données de CI, puis exécutez les rapports CA CMDB.
2. Redémarrez le service Serveur CA Cohesion ACM.
3. Utilisez un serveur CA CMDB cible différent pour exporter les données de Ci et exécutez les rapports CA CMDB.
4. (Facultatif) Répétez les étapes 2 et 3.

Configuration de l'interface Web

Quand vous installez CA SDM, l'*interface Web* (communément appelée *interface de navigation*) est automatiquement installée et vous pouvez la configurer dans le cadre de l'installation.

Sélectionnez le serveur Web selon la configuration de CA SDM. Examinez les deux cas suivants :

- Conventionnelle : lorsque le serveur Web et le serveur principal sont sur le même ordinateur, aucune action supplémentaire n'est requise. Toutefois, si vous utilisez un serveur Web et que le serveur principal est installé sur un ordinateur différent, installez et configurez les serveurs principal et secondaire.
- Disponibilité avancée : lorsque le serveur Web et le serveur principal sont sur le même ordinateur, aucune action supplémentaire n'est requise. Toutefois, si vous utilisez un serveur Web et que le serveur principal est installé sur un ordinateur différent, installez et configurez les serveurs d'arrière-plan et d'applications. L'interface Web pour les utilisateurs finals n'est jamais hébergée par le serveur d'arrière-plan. L'interface Web doit être hébergée uniquement sur les serveurs d'applications.

Sélectionnez l'ordinateur sur lequel le serveur Web réside et sur lequel vous prévoyez d'installer et de configurer l'interface Web à partir des serveurs CA SDM suivants, selon votre configuration de CA SDM :

- Conventionnelle : serveur secondaire. Installez ce serveur après avoir installé le serveur principal.
- Disponibilité avancée : serveur d'applications Installez ce serveur une fois le serveur d'arrière-plan installé.

Important : Par défaut, Tomcat est le serveur Web par défaut. Si vous voulez utiliser IIS comme serveur Web, configurez le produit manuellement et sélectionnez IIS. Pour de plus amples renseignements, reportez-vous à l'*Aide en ligne relative à la configuration du serveur*.

Pour configurer l'interface Web, effectuez les opérations suivantes :

1. (Obligatoire) Sous Windows ou UNIX, activez le moteur Web sur le serveur secondaire.
2. (Obligatoire) Configurez l'interface Web (page 245).

   Vous pouvez ensuite démarrer l'interface Web (page 246).

Ajout de moteurs Web ou de directeurs Web

Les moteurs Web se connectent à un gestionnaire d'objets pour traiter l'ensemble des demandes envoyées aux objets CA SDM. Les directeurs Web sont facultatifs et sont utilisés lorsque plusieurs moteurs Web sont installés sur un serveur unique. Vous pouvez configurer des directeurs Web sur tout serveur. Selon votre type de configuration, CA SDM installe un moteur Web par défaut sur les serveurs suivants :

- Conventionnelle : serveur principal
- Disponibilité avancée : tous les serveurs

1. Sous l'onglet Administration, sélectionnez Systèmes, Configurations.

   La page Liste des configurations s'affiche.
2. Sélectionnez la configuration à laquelle vous voulez ajouter le moteur ou le directeur Web.

   La page Détail de la configuration s'affiche.

   Remarque : Si c'est la première fois que vous modifiez la configuration, vous devrez d'abord créer une configuration. Si vous souhaitez modifier la configuration, il est recommandé de toujours créer une configuration ou de copier une configuration existante. Ce processus vous permet de rétablir la configuration précédente, si nécessaire.

3. Sélectionnez l'onglet Moteurs/directeurs Web.

   La page Liste des moteurs/directeurs Web s'ouvre et répertorie les moteurs et directeurs Web configurés pour le serveur.

   - Conventionnelle : un moteur Web existe par défaut sur le serveur principal. Vous pouvez ajouter des directeurs Web sur tout serveur.
   - Disponibilité avancée : il existe un moteur Web par défaut sur tous les serveurs. Vous pouvez ajouter plusieurs directeurs Web sur tout serveur CA SDM.

4. Cliquez sur Ajouter un moteur/directeur Web.

   La page Créer un moteur/directeur Web s'ouvre.

5. Remplissez les champs suivants :

   Important : Pour les langues localisées, entrez uniquement des caractères anglais dans les champs de saisie.

   Nom d'hôte

   Spécifie le nom d'hôte pour le moteur Web ou le directeur Web. Vous pouvez cliquer sur Rechercher pour chercher les serveurs.

   Pour un type de configuration de disponibilité avancée, le nom d'hôte est en lecture seule. Ce champ est rempli automatiquement en fonction du nom d'hôte que vous avez spécifié lors de la création de la configuration.

   Type

   Spécifie si vous configurez un moteur Web ou un directeur Web. Selon l'option sélectionnée, les champs pertinents sont automatiquement remplis.

   - Sélectionnez Moteur Web si vous voulez configurer un moteur Web.
   - Sélectionnez Directeur Web si vous voulez configurer un directeur Web.

   Remarque : Assurez-vous d'avoir sélectionné l'option appropriée, car vous ne pouvez pas modifier le type de processus après avoir enregistré la configuration.

Directeur Web

Spécifie le directeur Web qui est affecté au moteur Web. Vous pouvez cliquer sur Rechercher pour chercher les directeurs Web ajoutés au serveur.

Remarque : Lors de la mise en oeuvre d'un schéma d'équilibrage de la charge de moteur Web, d'une connexion SSL ou des deux, au moins deux moteurs Web doivent être affectés au même directeur Web.

Nom de l'interface CGI

Spécifie le nom unique de l'interface CGI pour le moteur Web. Cette valeur correspond au nom d'un exécutable CGI réel lorsqu'IIS ou Apache est utilisé en tant que serveur HTTP. Elle correspond à un paramètre de servlet lorsque Tomcat est utilisé en tant que serveur HTTP.

Exemples : (moteurs Web) pdmweb1, pdmweb2, (directeurs Web) pdmweb_d1 et pdmweb_d2.

Valeur par défaut : pdmweb.exe (le nom de CGI doit être unique).

Numéro de port CGI

Spécifie le port auquel les clients Web CA SDM peuvent se connecter. Le numéro de port de l'interface CGI est le même que celui sur lequel s'exécute le serveur Tomcat.

Valeur par défaut : 8080

Protocole

Spécifie le protocole pour accéder au moteur Web.

- Sélectionnez HTTPS si le moteur Web est configuré pour gérer toutes les demandes d'authentification d'utilisateur de client Web CA SDM.
- Sélectionnez HTTP si le moteur Web est configuré pour gérer toutes les demandes d'authentification non utilisateur de client Web (après l'authentification de l'utilisateur par le biais du moteur Web de connexion sécurisée).

État de l'enregistrement

Spécifie si le moteur Web ou le directeur Web est activé ou désactivé.

Remarque : Avant de définir l'état d'enregistrement d'un directeur Web sur Désactivé, supprimez le lien entre le directeur Web et les moteurs Web associés.

Gestionnaire d'objets

Spécifie le gestionnaire d'objets que vous voulez affecter au moteur Web.

Par défaut

Indique que le gestionnaire d'objets par défaut est affecté au moteur Web.

Non spécifié

Indique que le moteur Web peut se connecter à un gestionnaire d'objets disponible avec une valeur de disponibilité plus importante. La valeur de disponibilité correspond à la disponibilité du serveur à accepter de nouveaux clients. Une valeur de disponibilité égale à zéro signifie que le moteur Web n'accepte aucune session.

Sélectionner

Permet de spécifier un gestionnaire d'objets pour le moteur Web. Sélectionner cette option vous permet d'ajouter plusieurs gestionnaires d'objets ou des alias à la configuration.

6. Cliquez sur Enregistrer.

Le moteur Web ou le directeur Web que vous avez ajouté s'affiche dans la Liste des moteurs/directeurs Web.

Configuration de l'interface Web

Si la configuration par défaut spécifiée pour l'interface Web pendant l'installation de CA SDM ne correspond pas à vos exigences, modifiez le fichier *web.cfg*, situé dans le répertoire *répertoire-installation*\bopcfg\www. Modifiez le fichier à l'aide d'un éditeur de texte qui n'ajoute pas de caractères de formatage ou de contrôle, comme le Bloc-Notes ou WordPad.

Chaque entrée du fichier consiste en une ligne unique contenant un nom de propriété, éventuellement suivi d'une valeur. Les lignes commençant par le signe dièse (#) sont traitées comme des commentaires et sont donc ignorées.

Remarque : Pour plus d'informations sur les entrées du fichier web.cfg, reportez-vous au *Manuel d'administration*.

Démarrage de l'interface Web

Avant de pouvoir démarrer l'interface Web et utiliser CA SDM, vous devez veiller à ce que les services du serveur de démons et le serveur de base de données soient démarrés. Si vous avez configuré un serveur secondaire (par exemple, si l'interface Web est installée sur un serveur Web résidant sur un ordinateur autre que le serveur principal), vous devez exécuter l'utilitaire de surveillance du démon distant avant de démarrer le service du serveur principal.

- (Windows) Pour démarrer les services, ouvrez le panneau de configuration (Outils d'administration, Services). Puis, cliquez avec le bouton droit de la souris sur l'utilitaire de surveillance du démon distant de CA SDM et sélectionnez Démarrer.
- (Linux) Pour démarrer les services, ouvrez une invite de commande et exécutez la commande *pdm_client*.

Après avoir démarré les services, vous pouvez démarrer l'interface Web. La manière de démarrer l'interface Web dépend du type de serveur à partir duquel vous la démarrez (principal ou secondaire) et de l'utilisation éventuelle d'IIS. Vous pouvez aussi démarrer l'interface Web à partir d'un site Web interne.

- Pour démarrer l'interface Web, sélectionnez Démarrer, Tous les Programmes, CA, CA Service Desk Manager, Service Desk Manager Web Client.
- Pour démarrer l'interface Web à partir d'un ordinateur qui n'est pas le serveur principal ou un serveur secondaire, ouvrez un navigateur Web et entrez l'URL suivante :

  `http://servername:8080/CAisd/pdmweb.exe`

  Dans cette URL, *servername* correspond au nom de l'ordinateur qui héberge le serveur Web CA SDM.
- Pour démarrer l'interface Web à partir d'un ordinateur qui n'est pas le serveur principal ou un serveur secondaire, et si vous utilisez IIS comme serveur Web, ouvrez un navigateur Web et entrez l'URL suivante :

  `http://servername/CAisd/pdmweb.exe`
- Pour démarrer l'interface Web d'un site Web interne, ajoutez */pdmweb.exe* à l'URL de vos pages Web. Utilisez l'exemple de code HTML suivant comme guide :

  `A HREF=http://<server-name>:<port-no>/CAisd/pdmweb.exe`

  Dans cette URL, *server-name* identifie votre ordinateur et *port-no* est le port d'écoute de votre serveur Web.

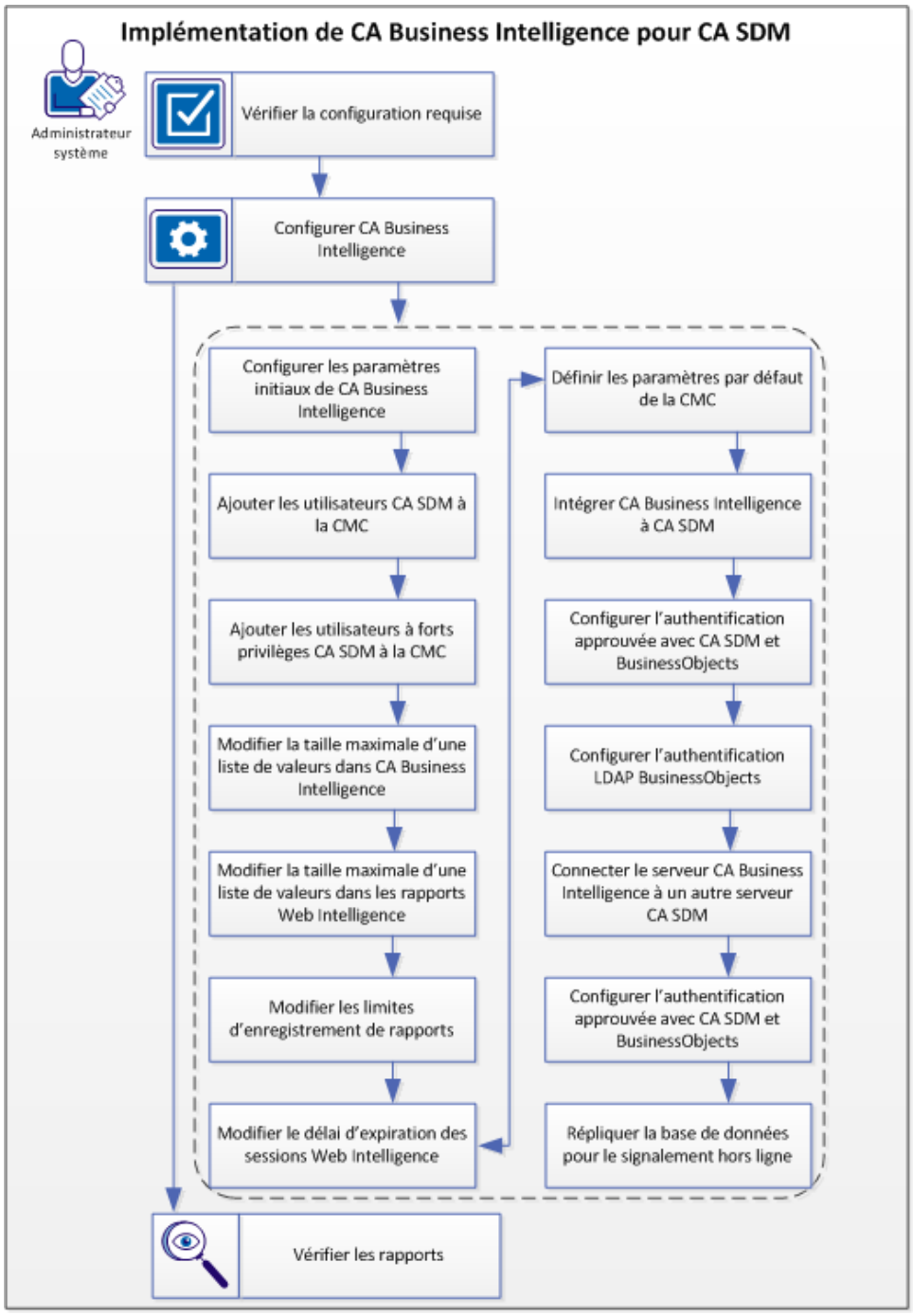
  Remarque : Si la sécurité de votre navigateur Internet Explorer est définie sur Elevée, un message d'avertissement lié au contenu s'affiche lorsque vous démarrez l'interface Web. Pour éviter ce message, ajoutez le site Web à vos sites fiables ou baissez vos paramètres de sécurité.

  Dans le cas de la disponibilité avancée, l'interface Web par défaut est facilement disponible avec l'installation par défaut et la configuration.

Mise en oeuvre de CA Business Intelligence pour CA SDM

CA Business Intelligence est un ensemble de logiciels de signalement et d'analyse utilisé par CA SDM pour présenter des données et appuyer des décisions opérationnelles. CA SDM utilise CA Business Intelligence pour intégrer, analyser, puis présenter les données à travers diverses options de signalement. Pour générer des rapports à partir de CA SDM, vous devez en tant qu'administrateur installer, configurer et intégrer CA Business Intelligence à CA SDM.

Le schéma suivant présente la mise en oeuvre de CA Business Intelligence pour CA SDM :


Implémentation de CA Business Intelligence pour CA SDM
Administrateur système
Vérifier la configuration requise
Configurer CA Business Intelligence
Configurer les paramètres initiaux de CA Business Intelligence
Ajouter les utilisateurs CA SDM à la CMC
Ajouter les utilisateurs à forts privilèges CA SDM à la CMC
Modifier la taille maximale d'une liste de valeurs dans CA Business Intelligence
Modifier la taille maximale d'une liste de valeurs dans les rapports Web Intelligence
Modifier les limites d'enregistrement de rapports
Modifier le délai d'expiration des sessions Web Intelligence
Définir les paramètres par défaut de la CMC
Intégrer CA Business Intelligence à CA SDM
Configurer l'authentification approuvée avec CA SDM et BusinessObjects
Configurer l'authentification LDAP BusinessObjects
Connecter le serveur CA Business Intelligence à un autre serveur CA SDM
Configurer l'authentification approuvée avec CA SDM et BusinessObjects
Répliquer la base de données pour le signalement hors ligne
Vérifier les rapports

1. Consultez les remarques sur le signalement. (page 249)
2. Configurez CA Business Intelligence. (page 249)
3. Vérifiez les rapports. (page 267)

Vérification des configurations requises

Avant de planifier la mise en oeuvre de CA Business Intelligence pour CA SDM, prenez connaissance des remarques suivantes :

- CA SDM r12.9 utilise la version 3.3 de CA Business Intelligence.
- L'installation de CA Business Intelligence requiert l'installation du serveur de gestion centralisée (CMS) sur le port 6400.
- Avant d'utiliser les rapports, les utilisateurs de CA SDM nécessitant un accès aux rapports doivent être ajoutés à la liste des administrateurs du CMS.
- Pour installer et configurer CA Business Intelligence, il est recommandé que les utilisateurs de SAP BusinessObjects disposent d'une installation existante de BusinessObjects.
- Si vous utilisez Firefox pour afficher les rapports, reportez-vous aux *Notes de parution de CA SDM* pour vérifier la version recommandée.
- Pour connaître la version de JRE prise en charge, reportez-vous aux Notes de parution de CA SDM.
- Crystal Reports Explorer et Desktop Intelligence ne sont pas pris en charge avec CA SDM.
- Si vous utilisez la configuration de disponibilité avancée, vous devez disposer d'un serveur distinct pour installer CA Business Intelligence.

Configuration de CA Business Intelligence.

Une fois installé, vous pouvez configurer CA Business Intelligence. Vous devez configurer des paramètres obligatoires pour générer des rapports à partir de CA SDM. Avant d'intégrer CA Business Intelligence à CA SDM, certaines configurations obligatoires, telles que l'ajout d'utilisateurs et les paramètres de sécurité, sont requises.

1. Configurez les paramètres de CA Business Intelligence.
2. Configurez des valeurs de plage de données et des paramètres de jointure.
3. Ajoutez des utilisateurs et des groupes CA SDM.
4. Ajoutez le compte d'utilisateur à forts privilèges CA SDM par défaut.
5. Modifiez les paramètres de sécurité par défaut et de Web Intelligence.
6. Intégrez CA Business Intelligence à CA SDM.
7. Configurez l'authentification approuvée pour BusinessObjects et CA SDM.
8. (Facultatif) Configurez l'authentification LDAP BusinessObjects.
9. (Applicable à la configuration conventionnelle uniquement) Connectez le serveur CA Business Intelligence à un serveur CA SDM différent.
10. Modifiez la taille maximale d'une liste de valeurs.
11. Modifiez la temporisation de session de Web Intelligence.

Configurez les paramètres initiaux de CA Business Intelligence

Cette étape charge l'univers et les rapports de CA SDM, crée des groupes et éventuellement crée un utilisateur pour chaque groupe et établit des autorisations de groupe.

1. Insérez le support d'installation DVD 2 dans le lecteur du serveur CA Business Intelligence. Si le menu d'installation ne s'affiche pas automatiquement, démarrez l'installation en double-cliquant sur le fichier setup.exe, situé à la racine du support d'installation.

   Remarque : Si votre ordinateur ne dispose pas d'un lecteur approprié pour le support d'installation, copiez le contenu du support sur l'ordinateur sur lequel vous souhaitez installer CA Business Intelligence. Démarrez ensuite la configuration. Pour une configuration distante sur le réseau, vous pouvez partager un lecteur ou dossier sur le réseau et vous y connecter pour démarrer la configuration.

2. Pour sélectionner votre langue dans la liste, cliquez sur Sélectionner une langue.

   Le menu d'installation s'affiche.

3. Cliquez sur l'onglet Installer le produit.

4. Cliquez sur Configuration de CA Business Intelligence.
5. Remplissez les champs suivants pour la configuration de CA Business Intelligence :

   Nom de l'administrateur BI

   Indique le nom d'un utilisateur de CA Business Intelligence qui appartient au groupe Administrateurs. Le nom de l'utilisateur est Administrateur pour une nouvelle installation de CA Business Intelligence.

   Mot de passe de l'administrateur BI

   Indique le mot de passe de l'administrateur de CA Business Intelligence.

   Nom de l'administrateur du centre de services

   Indique le nom de l'administrateur de CA SDM.

   Mot de passe de l'administrateur du centre de services

   Indique le mot de passe de l'utilisateur à forts privilèges de CA SDM.

   Créer des utilisateurs par défaut

   Crée des groupes par défaut et des utilisateurs correspondants dans CA Business Intelligence.

   Si vous avez installé CA Business Intelligence sur un autre ordinateur que CA SDM, les champs suivants apparaissent dans la configuration de CA Business Intelligence :

   Hôte principal du centre de services

   Indiquez le nom d'hôte du serveur CA SDM selon la configuration :

   - Conventionnelle : serveur principal
   - Disponibilité avancée : serveur d'applications

   Port ODBC

   Spécifie le numéro de port du pilote ODBC pour CA SDM.

   Recommandé : 19987.

   Emplacement d'installation ODBC

   Spécifie l'emplacement personnalisé pour l'installation ODBC s'il est différent de l'emplacement par défaut.

6. Vérifiez la configuration de CA Business Intelligence.

Configuration des paramètres de basculement

Ce processus est uniquement applicable à la configuration de disponibilité avancée. Lorsque plusieurs serveurs d'applications sont configurés, vous pouvez configurer des paramètres de basculement. Configurez le basculement pour rediriger des sessions d'utilisateur actives vers l'autre serveur d'applications. Vous pouvez également configurer l'équilibrage de charge entre plusieurs serveurs d'applications.

1. Appelez l'invite de commande en tant qu'administrateur.
2. Exécutez odbcad32.exe à partir de l'emplacement C:\Windows\SysWOW64 sur le serveur CA Business Intelligence.

   La boîte de dialogue DataDirect OpenAccess SDK ODBC Driver Setup s'affiche.

   Remarque : Le chemin d'accès spécifié est valide pour l'installation sous Windows 64 bits.
3. Entrez les détails du serveur d'applications sous l'onglet General.
4. Sous l'onglet Failover, entrez les détails de l'autre serveur d'applications, à l'aide de la syntaxe suivante :

   (Host=AppServer1:Port=19987,Host=AppServer2:Port=19987,..)
5. Pour répartir la charge entre les serveurs, sélectionnez Load Balancing. La charge est équilibrée entre les serveurs dont les détails sont indiqués sous l'onglet General et ceux dont les détails sont indiqués sous l'onglet Failover. Les serveurs sont sélectionnés de manière aléatoire.

   Remarque : Pour configurer le basculement ou l'équilibrage de la charge, sélectionnez Force SQL_DRIVER_NOPROMPT.
6. Cliquez sur Apply, puis sur OK.

   Vous avez configuré les paramètres de post-configuration pour la configuration de disponibilité avancée.

Configuration des valeurs de période et des paramètres de jointure

Après l'installation de CA Business Intelligence, effectuez les opérations suivantes :

- Configurez les valeurs de période pour que les filtres de période de CA Business Intelligence fonctionnent correctement.
- Configurez les paramètres de jointure pour que les jointures externes d'univers soient prises en charge.

1. Sur l'ordinateur sur lequel CA Business Intelligence a été installé , accédez à l'emplacement suivant :

   ```
   C:\Program Files\CA\SC\CommonReporting3\BusinessObjects Enterprise 12.0\win32_x86\dataAccess\connectionServer\odbc\
   ```

2. Pour configurer les valeurs de période, ouvrez le fichier odbc.prm à l'aide d'un éditeur de texte et accédez à la section <Configuration>, puis recherchez la ligne suivante :

   ```
   <Parameter Name="USER_INPUT_DATE_FORMAT">{\d 'yyyy-mm-dd'}</Parameter>
   ```

3. Modifiez la ligne comme suit pour y inclure "hh:mm:ss am/pm" :

   ```
   <Parameter Name="USER_INPUT_DATE_FORMAT">{\d 'yyyy-mm-dd hh:mm:ss am/pm'}</Parameter>
   ```

4. Recherchez la ligne suivante pour configurer les paramètres de jointure :

   ```
   <Parameter Name="EXT_JOIN">NO </Parameter>
   ```

5. Modifiez la ligne pour remplacer NO par YES, comme suit :

   ```
   <Parameter Name="EXT_JOIN">YES</Parameter>
   ```

6. Recherchez la ligne suivante :

   ```
   <Parameter Name="OUTERJOINS_GENERATION">NO</Parameter>
   ```

7. Modifiez la ligne pour remplacer NO par FULL_ODBC, comme suit :

   ```
   <Parameter Name="OUTERJOINS_GENERATION">FULL_ODBC</Parameter>
   ```

8. Ajoutez les 3 lignes suivantes après le paramètre OUTERJOINS_GENERATION :

   ```
   <Parameter Name="LEFT_OUTER"></Parameter> <Parameter Name="RIGHT_OUTER"></Parameter> <Parameter Name="OUTERJOINS_COMPLEX">Y</Parameter>
   ```

9. Enregistrez le fichier odbc.prm.

10. Redémarrez les services BusinessObjects Enterprise.

    Les valeurs de période et les paramètres de jointure sont désormais configurés. Les filtres de période fonctionnent avec CA Business Intelligence et les jointures externes d'univers sont prises en charge.

Ajout de vos utilisateurs CA SDM à la CMC

La console de gestion centrale (CMC) est un utilitaire administratif qui vous permet de contrôler l'accès des utilisateurs à InfoView et à d'autres applications BusinessObjects. Avec la CMC, vous pouvez affecter des autorisations d'accès utilisateur et de sécurité à des dossiers et documents.

Remarque : Pendant la phase de configuration, une case à cocher facultative indique si des exemples d'utilisateurs sont ajoutés à la CMC. Si vous avez sélectionné cette option, votre CMC contient plusieurs exemples d'utilisateurs. Vous pouvez utiliser ces exemples comme modèles lors de la définition des autorisations utilisateur et des options d'authentification pour votre environnement de signalement. Pour de plus amples renseignements sur les exemples d'utilisateurs, reportez-vous au *Manuel d'administration*.

1. Dans le menu Démarrer du serveur CA Business Intelligence, sélectionnez BusinessObjects XI Release 3.1, BusinessObjects Enterprise, BusinessObjects Enterprise Console de gestion centrale.

   La page Console de gestion centrale (CMC) s'ouvre.

2. Entrez le nom et le mot de passe de l'utilisateur à forts privilèges.
3. Dans la liste Type d'authentification, sélectionnez Entreprise.
4. Cliquez sur Connexion.

   La page d'accueil de la CMC s'ouvre.

5. Cliquez sur Utilisateurs et Groupes dans la section Organiser de la page d'accueil de la CMC.
6. Cliquez sur Gérer, Nouveau, Nouvel utilisateur.

   La boîte de dialogue Nouvel utilisateur s'ouvre.

7. Sélectionnez Entreprise dans la liste Type d'authentification.
8. Sous Nom du compte, spécifiez l'ID d'utilisateur de CA SDM.
9. Sous l'onglet Propriétés, spécifiez vos données et vos paramètres de mot de passe comme suit :

   Mot de passe

   Entrez le mot de passe, puis confirmez-le. Ce mot de passe correspond au mot de passe de l'utilisateur CA SDM. La longueur maximale du mot de passe est de 64 caractères.

Ce mot de passe doit inclure des minuscules et des majuscules, comporter au moins six caractères et ne peut pas contenir le mot administrateur sous quelque forme que ce soit. Il doit également contenir au moins deux des types de caractères suivants.

- Majuscules
- Minuscules
- Chiffres
- Ponctuation

Password never expires

Cochez la case.

User must change password at next logon

Cette case est cochée par défaut. Si vous ne souhaitez pas obliger les utilisateurs à modifier leur mot de passe lorsqu'ils se connectent pour la première fois, décochez cette case.

10. Pour limiter l'accès aux données des rapports à l'aide de la partition de données et des contraintes de propriété, cochez la case Enable Database Credentials for Business Objects Universes. Dans les champs qui s'affichent, spécifiez le nom de compte et le mot de passe de l'utilisateur CA SDM, puis confirmez le mot de passe.
11. Cliquez sur Actions, Membres de pour spécifier les groupes auxquels l'utilisateur doit appartenir.
12. Cliquez sur Joindre le groupe pour afficher les groupes disponibles. Par défaut, l'utilisateur est membre du groupe Everyone.
13. Dans la zone Groupes disponibles, sélectionnez un ou plusieurs groupes supplémentaires.
14. Cliquez sur la flèche > pour ajouter le ou les groupes.
15. Cliquez sur OK.

    La boîte de dialogue Membres de apparaît et répertorie les groupes dont fait partie l'utilisateur.

Remarque : Pour de plus amples renseignements sur l'ajout d'utilisateurs et de groupes et sur la configuration de la sécurité des partitions de données, reportez-vous au *Manuel d'administration.*

Ajout de l'utilisateur à forts privilèges CA SDM à la CMC

La connexion CA SDM Universe est configurée par défaut pour utiliser le nom d'utilisateur et le mot de passe CA SDM lors de l'accès aux données. Ce compte d'utilisateur est ajouté à la CMC comme nouvel utilisateur de CA Business Intelligence. Vous avez besoin de cet utilisateur si vous prévoyez de configurer la sécurité de la partition de données pour le signalement et pour tester les rapports de l'onglet Rapports. L'onglet Rapports requiert un utilisateur qui est défini auprès de CA SDM et de CA Business Intelligence.

1. Cliquez sur la zone de gestion Utilisateurs et groupes de la CMC.
2. Sous Nom du compte, sélectionnez le compte de l'utilisateur à forts privilèges CA SDM.
3. Sous l'onglet Propriétés, spécifiez les données relatives à votre mot de passe.
4. Sélectionnez la case à cocher Enable Database Credentials for Business Objects Universes. Dans les champs qui s'affichent, spécifiez le nom de compte et le mot de passe de l'utilisateur à forts privilèges, puis confirmez le mot de passe.
5. Cliquez sur l'onglet Membres de pour spécifier le groupe auquel l'utilisateur à forts privilèges appartient.
6. Cliquez sur le bouton Joindre le groupe pour afficher les groupes disponibles.
7. Dans la zone Groupes disponibles, sélectionnez Administrateurs et CA Universe Developer (Développeur d'univers CA).
8. Cliquez sur la flèche > pour ajouter ces groupes.
9. Cliquez sur OK.

   L'onglet Membre de apparaît et répertorie les groupes auxquels l'utilisateur appartient.

Modification de la taille maximale d'une liste de valeurs dans CA Business Intelligence

Lors de l'installation de CA Business Intelligence, le nombre maximal de valeurs pouvant être renvoyées par lot pour une liste de valeurs dans les rapports Crystal est automatiquement fixé à 5 000 enregistrements de la base de données. Pour des raisons de performance, vous pouvez modifier la taille pour que la liste des valeurs renvoyées à l'utilisateur soit en plusieurs lots de la taille spécifiée ou plus petits.

Remarque : Pour de plus amples renseignements sur l'amélioration des performances du serveur de rapports Web Intelligence, reportez-vous à la documentation de BusinessObjects.

1. Créez la clé de registre suivante :

   HKEY_CURRENT_USER\SOFTWARE\Business Objects\Suite 12.0\CrystalReports\DatabaseOptions\LOV

   Remarque : La clé de registre créée remplace les paramètres de la clé de registre HKEY_LOCAL_MACHINE\SOFTWARE\Business Objects\Suite 12.0\CrystalReports\DatabaseOptions\LOV.

2. Ajoutez une valeur de chaîne comme MaxRowsetRecords.

3. Définissez la valeur MaxRowsetRecords sur le nombre maximal de valeurs requises pour le rapport. Par exemple, une valeur de 2000 renvoie jusqu'à 2 000 valeurs du plus bas niveau d'un paramètre de cascade.

   Remarque : La valeur zéro (Illimité) ne fonctionne pas avec BusinessObjects Enterprise ou Crystal Reports Server. Il faut plus de temps pour remplir les valeurs si elles sont définies sur zéro, c'est-à-dire, sur la liste de valeurs maximales, lorsque vous accédez à un rapport Crystal Report à partir d'InfoView.

4. Redémarrez le service ou l'application concernée, le cas échéant.

Remarque : Ces clés de registre n'affectent pas la liste de valeurs renvoyée lorsqu'un rapport est basé sur un univers.

Modification de la taille maximale d'une liste de valeurs dans les rapports Web Intelligence

Lors de l'installation de CA Business Intelligence, le nombre maximal de valeurs pouvant être renvoyées par lot pour une liste de valeurs dans les rapports Web Intelligence est automatiquement fixé à 5 000 enregistrements de la base de données. Pour des raisons de performance, vous pouvez modifier la taille pour que la liste des valeurs renvoyées à l'utilisateur soit en plusieurs lots de la taille spécifiée ou plus petits.

Remarque : Pour de plus amples renseignements sur l'amélioration des performances du serveur de rapports Web Intelligence, reportez-vous à la documentation de BusinessObjects.

1. Connectez-vous à la console de gestion centrale.
2. Cliquez sur Serveurs.
3. Cliquez avec le bouton droit de la souris sur le serveur de traitement Web Intelligence et sélectionnez Propriétés.

4. Augmentez la valeur de la taille maximale d'une liste de valeurs (entrées).
5. Enregistrez et redémarrez le serveur de traitement Web Intelligence.

   Remarque : La définition d'un nombre élevé pour la taille maximale d'une liste de valeurs (entrées) peut affecter les performances de Web Intelligence. Il est recommandé de définir un nombre approprié en fonction des performances système.

Modification des limites d'enregistrement de rapport

Lorsque vous installez CA Business Intelligence, le nombre d'enregistrements que le serveur récupère de la base de données lorsqu'un utilisateur exécute une requête ou un rapport dans Crystal reports est automatiquement fixé à 20 000 enregistrements. Vous pouvez modifier le paramètre pour que les utilisateurs qui exécutent les rapports reçoivent les ensembles d'enregistrements qu'ils attendent.

Remarque : Pour des détails complets sur les tâches d'administration que vous pouvez effectuer pour le serveur de la page Crystal Reports, reportez-vous à la documentation de BusinessObjects.

1. Avec BusinessObjects Enterprise, connectez-vous à la CMC.
2. Accédez à la page affichant les serveurs.
3. Cliquez sur le serveur de la page Crystal Reports.
4. Sous l'onglet Propriétés, modifiez le paramètre pour le champ Database Records To Read When Previewing or Refreshing a Report pour spécifier soit un nombre illimité d'enregistrements, soit une limite d'enregistrements.
5. Cliquez sur Appliquer.
6. Redémarrez le serveur de la page Crystal Reports.

   La limite d'enregistrement de rapport est modifiée et elle est utilisée lors de l'exécution des rapports.

Modification de la temporisation de session de Web Intelligence

Par défaut, les utilisateurs disposent d'un accès Contrôle total à l'application Web Intelligence.

Par défaut, l'application Web Intelligence présente une temporisation de session de 20 minutes. Les rapports non enregistrés sont perdus lorsque la session expire et l'utilisateur doit se connecter à nouveau pour utiliser l'application.

Les administrateurs peuvent modifier la valeur de temporisation de la session de connexion à l'aide de la console de gestion centrale (CMC).

1. Sur la page d'accueil de la CMC, sélectionnez Serveurs.

   La fenêtre Serveurs s'ouvre.

2. Dans la colonne Nom du serveur, sélectionnez Web_IntelligenceReportServer.
3. Entrez la valeur de temporisation appropriée (nombre de minutes) dans le champ Connection Time Out (Expiration de la connexion).
4. Cliquez sur Appliquer.

   Vos modifications prennent effet après le redémarrage du serveur.

5. Cliquez sur OK.

   La valeur de temporisation de la session de connexion est définie.

Paramètres par défaut dans la CMC

La plupart de la configuration du signalement est effectuée silencieusement pendant l'installation de CA Business Intelligence. La configuration du signalement implique les actions suivantes :

- Configuration de la sécurité
- Déploiement des rapports
- Déploiements des univers
- Déploiement des objets de programme
- Configuration des paramètres Web Intelligence

L'administrateur peut à tout moment se connecter à la CMC de BusinessObjects et modifier les paramètres par défaut. Les utilisateurs disposent d'autorisations d'accès en fonction du groupe CA SDM auquel ils appartiennent.

Remarque : Pour de plus amples renseignements sur la CMC BusinessObjects, reportez-vous au *Manuel de mise en oeuvre CA Business Intelligence*.

Intégration de CA Business Intelligence à CA SDM

Après avoir installé CA Business Intelligence, actualisez les options de signalement Web afin que CA SDM soit correctement intégré avec CA Business Intelligence.

1. Sous l'onglet Administration, sélectionnez Gestionnaire d'options, Rapport Web.

   La liste des options s'affiche.

2. Définissez les valeurs correctes pour les options de rapports Web suivantes :

   bo_server_auth

   Spécifie le type d'authentification que vous souhaitez utiliser pour le signalement. Vous pouvez spécifier les types d'authentification suivants :

   - secEnterprise **:** (Par défaut) spécifiez Authentication Enterprise comme type d'authentification si vous préférez créer des comptes et des groupes distincts dans BusinessObjects afin de les utiliser dans CA Business Intelligence, ou si aucune hiérarchie d'utilisateurs n'a été configurée dans une base de données d'utilisateurs Windows NT, sur un serveur LDAP ou un serveur Windows AD.

     Remarque : Avant d'utiliser l'option secEnterprise, ajoutez vos utilisateurs de rapports CA SDM (page 254) à la CMC de BusinessObjects. Dans la console CMC, vous devez entrer les mêmes noms d'utilisateur et mots de passe que ceux configurés dans CA SDM.

   - secLDAP **:** spécifiez Authentification LDAP comme type d'authentification si vous avez déjà configuré un serveur d'annuaire LDAP et souhaitez utiliser vos comptes et groupes d'utilisateurs LDAP dans BusinessObjects avec CA Business Intelligence.

     Lorsque vous mappez les comptes LDAP à BusinessObjects, les utilisateurs peuvent accéder à CA Business Intelligence avec leur nom d'utilisateur et leur mot de passe LDAP. Grâce à cette configuration, il n'est plus nécessaire de recréer des comptes de groupes et d'utilisateurs dans BusinessObjects.

   - secWinAD **:** spécifiez Authentication Windows AD comme type d'authentification si vous travaillez dans un environnement Windows 2000 et que vous souhaitez utiliser vos comptes et groupes d'utilisateurs Active Directory (Répertoire actif) existants dans BusinessObjects avec CA Business Intelligence.

   - secExternal **:** spécifiez Authentification externe comme type d'authentification si vous intégrez la solution d'authentification BusinessObjects dans une solution d'authentification tierce (par exemple, en utilisant JCIFS avec Tomcat). Ce type d'authentification requiert la configuration Authentification approuvée dans BusinessObjects pour autoriser les utilisateurs à ouvrir une session sans fournir leurs mots de passe.

   Remarque : Pour de plus amples renseignements sur les options de sécurité alternatives, reportez-vous au *Manuel de mise en oeuvre de CA Business Intelligence*.

bo_server_cms

Spécifiez le nom du serveur de gestion centralisée (CMS) responsable de la gestion d'une base de données d'informations sur votre BusinessObjects, que vous utilisez avec CA Business Intelligence.

Pour bo_hostname, utilisez le nom d'hôte de l'ordinateur sur lequel CA Business Intelligence est installé. La valeur bo_cms_port par défaut est 6400.

Remarque : Pour obtenir des renseignements détaillés sur les options avancées de configuration du serveur, reportez-vous au *Manuel d'installation de CA Business Intelligence*.

bo_server_location

Spécifie le nom d'hôte de l'ordinateur sur lequel CA Business Intelligence est installé. Spécifiez bo_hostname. CA SDM utilise cette URL pour créer des URL de rapport afin de demander des rapports au serveur BusinessObjects. L'emplacement du serveur CMS est spécifié par le nom d'hôte et le port.

Remarque : Pour obtenir des renseignements détaillés sur chaque option, reportez-vous au *Manuel de mise en oeuvre de CA Business Intelligence*.

3. Cliquez sur Enregistrer, puis Actualiser.

   La page Détail des options est mise à jour avec votre sélection.

4. Cliquez sur Fermer la fenêtre.

5. Arrêtez le service appelé Serveur CA SDM, puis redémarrez-le.

   Les paramètres de signalement Web sont configurés correctement pour fonctionner avec CA SDM. Vous pouvez maintenant configurer des rapports Web.

   Remarque : Pour de plus amples renseignements sur la configuration des rapports Web, reportez-vous au *Manuel d'administration*.

Configuration de l'authentification approuvée avec CA SDM et BusinessObjects

L'authentification approuvée vous permet d'utiliser un formulaire Single Sign On lors de l'intégration de CA SDM et CA Business Intelligence. Single Sign On permet aux utilisateurs de se connecter au système sans devoir fournir un même mot de passe plusieurs fois au cours d'une session.

1. Installez et configurez CA SDM.
2. Installez et configurez CA Business Intelligence.
3. Connectez-vous à la CMC en tant qu'administrateur.
4. Accédez à la CMC pour définir l'authentification approuvée.
5. Créez les contacts CA SDM et les utilisateurs de BusinessObjects.

6. Installez les options de rapports Web CA SDM et fixez l'option bo_server_auth à Enterprise.

   Remarque : Pour de plus amples renseignements sur *bo_server_auth*, reportez-vous à l'*Aide en ligne*.

7. Mettez Tomcat Apache BusinessObjects en cycle.
8. Mettez le serveur CA SDM en cycle dans les services Windows.

Configurez l'authentification approuvée dans CA Business Intelligence

Pour configurer l'authentification approuvée pour CA Business Intelligence, il convient d'abord de modifier le fichier web.xml.

1. Connectez-vous à la CMC en tant qu'administrateur et accédez à la zone de gestion des authentifications.

   La page Enterprise s'affiche.

2. Au bas de la page, sélectionnez l'option Trusted Authentication is enabled avant de spécifier une chaîne de texte dans le champ Secret partagé.

   Remarque : Le secret partagé est utilisé pour créer un mot de passe d'authentification approuvée.

3. Entrez une valeur de temporisation pour vos demandes d'authentification approuvées.

   Remarque : La valeur de temporisation détermine combien de temps la base de données CMS attend l'appel IEnterpriseSession.logon() de l'application cliente.

4. Cliquez sur Mettre à jour.

   L'authentification approuvée est configurée.

Configurez l'authentification approuvée dans CA SDM

Pour configurer l'authentification approuvée dans CA SDM, il convient de modifier le fichier TrustedPrincipal.conf.

1. Ouvrez le fichier TrustedPrincipal.conf localisé dans le répertoire suivant :
   `NX_ROOT\bopcfg\www\CATALINA_BASE\webapps\CAisd`
2. Modifiez cette ligne
   `SharedSecret=<Secret partagé comme entré dans CMC>`

   comme suit :
   `SharedSecret=xxxx`
   `(xxxx correspondant au secret partagé entré dans la CMC à l'étape 3)`
3. Cliquez sur Enregistrer.
4. Répétez les étapes 1 à 3 pour tous les serveurs d'applications configurés.
5. Redémarrez le serveur Tomcat de CA Business Intelligence.

   L'authentification approuvée dans CA SDM est configurée.

Remarque : Vous devez configurer l'authentification approuvée dans le serveur d'arrière-plan CA SDM pour lancer des rapports à partir de l'URL de serveur d'arrière-plan.

Configuration de l'authentification LDAP BusinessObjects

Lors de la configuration de l'authentification LDAP, la valeur "cn" de l'information d'authentification de l'administrateur du serveur LDAP doit être le nom complet (prénom, nom). La configuration de l'authentification LDAP permet de mapper des attributs LDAP pour utiliser le nom de connexion de l'utilisateur final.

Important : Lors de la configuration de l'authentification LDAP, le Nom du compte d'utilisateur pour BusinessObjects doit correspondre à l'ID d'utilisateur du contact CA SDM.

1. Accédez à la zone de gestion des authentifications de la console de gestion centrale (CMC).
2. Double-cliquez sur LDAP.

3. Entrez le nom et le numéro de port de vos hôtes LDAP dans le champ Add LDAP host (nom_hôte:port). Par exemple, "myserver:123".
4. Cliquez sur Ajouter, puis sur OK.
5. Sélectionnez Personnalisé pour le type de serveur dans la liste des types de serveur LDAP.
6. Suivez les invites dans l'assistant de configuration CMS pour effectuer la configuration.

   L'authentification LDAP pour BusinessObjects est configurée.

Remarque : Pour de plus amples renseignements sur la configuration de l'authentification LDAP, consultez *l'Aide en ligne de CMS* et le manuel *BusinessObjects Enterprise Administrator's Guide*.

Connexion du serveur CA Business Intelligence à un serveur CA SDM différent

Cette opération est requise pour générer des rapports à partir d'une autre instance de CA SDM installée sur un serveur différent.

1. Créez un DSN ODBC pour le serveur CA SDM (page 264).
2. Connectez l'univers CA SDM à ce serveur CA SDM (page 265).

Création d'un DSN ODBC pour le serveur CA SDM

Utilisez l'Administrateur de sources de données ODBC pour créer un DSN ODBC.

1. Démarrez l'Administrateur de sources de données ODBC Windows (Sources de données (ODBC)).
2. Sur le formulaire Administrateur de sources de données ODBC, sélectionnez l'onglet DSN système, puis Ajouter.
3. Sur le formulaire Créer une nouvelle source de données, sélectionnez le pilote DataDirect OpenAccess, puis Terminer.
4. Sur le formulaire DataDirect OpenAccess ODBC 32 Setup, affectez un nom ODBC, puis sélectionnez Avancé.

   La convention d'affectation de noms à utiliser est casd_hostname. Par exemple, si le nom d'hôte du serveur CA SDM est MyServer, vous utilisez casd_MyServer.

5. Sur le formulaire Configuration de base de données OpenAccess, sélectionnez Ajouter.
6. Dans le formulaire Installation de base de données OpenAccess, entrez les renseignements suivants :
   - Nom : spécifiez casd_hostname.
   - Adresse IP : spécifiez l'adresse IP du serveur CA SDM.
   - Port : spécifiez 19987.
   - Type : sélectionnez SQL.
7. Cliquez sur OK.
8. Sur le formulaire Configuration de base de données OpenAccess, sélectionnez OK.
9. Sur le formulaire DataDirect OpenAccess ODBC 32 Setup, sélectionnez casd_hostname dans la liste déroulante Base de données, puis OK.

   Le DSN ODBC est créé.

Connexion de l'univers CA SDM au serveur

Utilisez Designer dans BusinessObjects Enterprise pour établir une connexion.

1. Dans le menu Démarrer, accédez à BusinessObjects XI Release 3.1, BusinessObjects Enterprise, Designer.
2. Connectez-vous à Designer avec les informations d'authentification suivante.
   - Système : spécifiez le nom d'hôte du serveur sur lequel CA Business Intelligence est installé.
   - Nom d'utilisateur : spécifiez le nom de l'administrateur de CA Business Intelligence (généralement Administrateur).
   - Mot de passe : spécifiez le mot de passe de l'administrateur de CA Business Intelligence.
   - Authentification : sélectionnez Enterprise.

   La fenêtre Designer s'affiche.
3. Cliquez sur Fichier, Importer.

   La boîte de dialogue Importation de l'univers s'affiche.
4. Sélectionnez le dossier CA Universes dans la liste déroulante, puis l'univers CA SDM et cliquez sur OK.

   Remarque : Si vous utilisez Designer pour la première fois, vous devrez peut-être d'abord utiliser la fonction Parcourir pour rechercher le dossier CA Universes.

5. Cliquez sur OK dans la zone de message Universe successfully imported (Univers importé correctement).

   La fenêtre de l'univers s'affiche.

6. Sélectionnez Fichier, Paramètres.

   La boîte de dialogue Paramètres de l'univers s'affiche.

7. Sous l'onglet Définition, cliquez sur Modifier.

   La boîte de dialogue Paramètres de connexion s'affiche.

8. Sélectionnez Modifier.

9. Sélectionnez le DSN ODBC que vous avez créé (casd_hostname) dans la liste déroulante Nom de la source de données et spécifiez les champs Nom d'utilisateur et Mot de passe à l'aide du nom d'utilisateur à forts privilèges et du mot de passe CA SDM.

10. Cliquez sur Suivant, Tester la connexion. Suivez ensuite les instructions des boîtes de dialogue Connexion à l'univers.

11. Cliquez sur OK pour terminer.

12. Sélectionnez Fichier, Exporter.

    La boîte de dialogue Exportation de l'univers apparaît.

13. Sélectionnez le dossier CA Universes dans la liste déroulante Domaine.

14. Sélectionnez Everyone dans la liste Groupes.

15. Cliquez sur OK.

    L'univers est exporté et la connexion au serveur est établie.

Base de données répliquée pour le signalement hors ligne

Pour gérer les problèmes de performances potentiels pouvant affecter les composants de signalement installés avec CA SDM, vous pouvez créer une base de données répliquée pour le signalement hors ligne.

Remarque : Pour de plus amples renseignements sur la création d'une base de données répliquée pour le signalement hors ligne, consultez les exemples de documentation et de scripts figurant dans le répertoire NX_ROOT\samples\reporting.

Vérification des rapports

Pour assurer la génération des rapports sans difficultés, vérifiez la configuration CA Business Intelligence.

1. Cliquez sur l'onglet Rapports.

   La page Rapport Web s'affiche.

2. Cliquez sur InfoView.

   La fenêtre Business Objects InfoView s'ouvre.

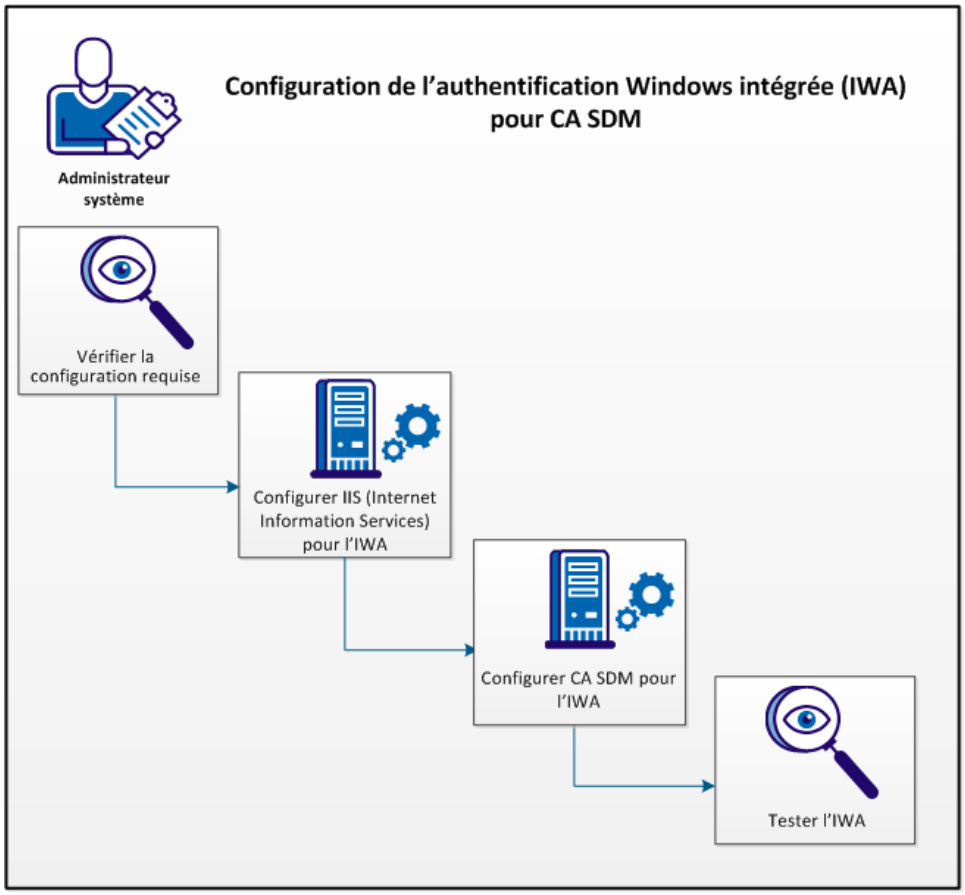
3. Cliquez sur le lien Liste des documents.
4. Développez Dossiers publics, CA Reports (Rapports CA), CA Service Desk (Centre de services CA).
5. Sélectionnez le dossier Actif dans le volet gauche.
6. Double-cliquez sur le rapport Liste des actifs.

   Le rapport renvoie un résultat de recherche supérieur ou égal à zéro. CA Business Intelligence est maintenant configuré pour CA SDM.

Configuration de l'authentification Windows intégrée pour CA SDM

En tant qu'administrateur système, vous pouvez authentifier les utilisateurs CA SDM grâce à une méthode d'authentification externe existante. Ce scénario décrit le processus permettant d'utiliser l'authentification Windows intégrée (IWA) pour authentifier les utilisateurs CA SDM par l'entremise de Microsoft Active Directory (Active Directory). Lorsque vous configurez des types d'accès CA SDM tels que des administrateurs pour utiliser IWA, les utilisateurs des types d'accès sélectionnés sont directement authentifiés à travers Active Directory.

Le schéma suivant illustre la configuration de l'IWA pour CA SDM :


Configuration de l'authentification Windows intégrée (IWA) pour CA SDM
Administrateur système
Vérifier la configuration requise
Configurer IIS (Internet Information Services) pour l'IWA
Configurer CA SDM pour l'IWA
Tester l'IWA

Pour configurer l'IWA pour CA SDM, effectuez les tâches suivantes :

1. Vérification de la configuration requise (page 269)
2. Configuration des services d'information Internet (IIS) pour IWA (page 270)
3. Configuration de CA SDM pour IWA (page 271)

4. Test d'IWA (page 271)

Vérification de la configuration requise

Avant de configurer l'authentification externe pour CA SDM, vérifiez la configuration requise suivante :

- Vous avez configuré des serveurs pour CA SDM.
- Vous avez installé IIS 7.0 sur le serveur suivant selon la configuration :
  - Configuration conventionnelle : serveur principal
  - Disponibilité avancée : serveur d'applications
- Vous avez configuré CA SDM pour utiliser IIS 7.0.
- Vous disposez de la liste des types d'accès pour lesquels l'authentification externe est requise. Par exemple : Administrateur CMDB, Employé et Utilisateur CMDB.

Configuration d'IIS pour IWA

Pour activer l'IWA, configurez le serveur IIS. La configuration modifie le mode d'authentification d'IIS, qui passe d'Anonyme à Authentification Windows. À l'issue de la configuration, le serveur commence à rediriger les demandes d'authentification vers la source externe.

1. Connectez-vous en tant qu'administrateur au serveur suivant, selon la configuration :
   - Conventionnelle : serveur principal ou secondaire
   - Disponibilité avancée : serveur d'arrière-plan.
2. Ouvrez Outils d'administration, Gestionnaire des services d'information Internet IIS.
3. Développez le noeud Nom de serveur, dans lequel Nom de serveur est celui du serveur CA SDM.
4. Développez Sites, Site Web par défaut, Noeud CAisd.

   La page d'accueil CAisd s'ouvre.
5. Double-cliquez sur l'icône Authentification.

   La page Paramètres d'authentification s'ouvre.
6. Pour désactiver l'authentification anonyme, cliquez sur Valeur de l'état actuelle.
7. Pour activer l'authentification Windows, cliquez sur Valeur de l'état actuelle.
8. Pour appliquer les changements, redémarrez l'IIS.

Vous avez configuré l'IIS pour IWA.

Configuration de CA SDM pour IWA

Configurez l'IWA pour chaque type d'accès sélectionné. Après la configuration d'un type d'accès pour l'authentification externe, CA SDM authentifie de façon externe les contacts de ce type d'accès.

Procédez comme suit :

1. Connectez-vous à CA SDM en tant qu'administrateur système.
2. Sélectionnez l'onglet Administration, Gestion des rôles et de la sécurité, Types d'accès.

   La page Liste des types d'accès s'ouvre.
3. Cliquez sur le type d'accès pour lequel l'authentification externe est requise.

   Le formulaire Mettre à jour le type d'accès s'ouvre.
4. Sélectionnez l'onglet Authentification Web et sélectionnez la case à cocher Autoriser l'authentification externe.
5. Dans la liste déroulante Type de validation, sélectionnez une valeur appropriée. Les valeurs suivantes requièrent une description :

   Aucun accès

   Spécifie que le type d'accès sélectionné n'est pas autorisé.

   Ouvert

   Spécifie que l'accès est autorisé pour tous les utilisateurs.

   Système d'exploitation

   Spécifie que l'information d'authentification du système d'exploitation du serveur CA SDM est requise pour accéder à CA SDM. Si vous avez configuré EEM, la demande de connexion serait redirigée vers le serveur EEM.

   NIP

   Spécifie que la valeur du champ d'enregistrement du contact CA SDM sélectionné est requise pour l'authentification. Par exemple, si vous choisissez NIP comme Type de validation et que vous sélectionnez Contact_Number dans la liste déroulante du champ NIP, le numéro de contact de l'utilisateur sera requis pour l'authentification.

   Remarque : Le type de validation n'est pas utilisé pour la validation d'IWA, mais il est utilisé lorsque l'utilisateur se connecte par l'entremise du formulaire de connexion CA SDM. La page Connexion CA SDM s'affiche uniquement lorsque l'utilisateur clique sur le lien Déconnexion ou que l'information d'authentification ne correspond pas à l'information d'authentification IIS.
6. Cliquez sur Enregistrer.

   Pour configurer l'authentification externe pour d'autres types d'accès, répétez les étapes 1 à 6.

Test d'IWA

Testez l'IWA avec un ID d'utilisateur dont l'enregistrement de contact correspondant se trouve dans CA SDM. Si vous pouvez vous connecter, cela signifie que l'IWA est correctement configurée.

1. Connectez-vous au serveur suivant selon la configuration, avec un ID d'utilisateur dont l'enregistrement de contact correspondant se trouve dans CA SDM :
   - Conventionnelle : serveur principal ou secondaire
   - Disponibilité avancée : serveur d'applications

   Remarque : Si les options LDAP ont été installées dans le gestionnaire d'options, vous pouvez également créer un contact dans CA SDM à partir d'un contact Active Directory (Répertoire actif).
2. Lancez le navigateur et entrez l'URL de CA SDM.

   La page d'accueil du centre de services s'ouvre.

Vous avez configuré l'IWA.

Exécution des politiques d'automatisation

Dans Gestion des connaissances, la fonctionnalité Politiques d'automatisation fournit un ensemble de politiques d'automatisation par défaut qui vous permettent de gérer plus efficacement les connaissances de votre organisation. Une politique d'automatisation décrit la condition qui permet de marquer les documents pour la correction et de les identifier pour la publication ou le retrait tout au long des diverses étapes du processus de cycle de vie du document. Par exemple, vous pouvez spécifier la politique par défaut de "correction des liens rompus" qui correspond aux documents trouvés dans la base de connaissances avec des liens rompus. La tâche de correction du problème peut être affectée à un analyste.

La page Liste des politiques d'automatisation contient les détails des politiques que vous pouvez gérer. Pour afficher cette page, sélectionnez l'onglet Administration, Connaissances, Politiques d'automatisation.

Chaque politique contient une requête stockée qui s'exécute en cas de correspondance des documents pendant le traitement. À l'issue du traitement, un rapport Politique de cycle de vie apparaît dans le tableau de résultats CA SDM. Pour afficher un rapport, sélectionnez Documents de connaissances, Politiques d'automatisation. Le tableau de résultats permet à l'analyste de gérer ses propres documents, et par défaut, à l'administrateur de gérer tous les documents de chaque rôle.

Pour mettre en oeuvre les rapports, vous devez exécuter un processus par lot avec le Planificateur de politiques d'automatisation. Le planificateur s'exécute sur le serveur CA SDM suivant, selon la configuration, et contient les données requises pour afficher les rapports.

- Conventionnelle : serveur principal ou secondaire
- Disponibilité avancée : serveur d'arrière-plan

Quand vous avez terminé, exécutez la fiche de rapport des connaissances (page 273).

Pour exécuter le Planificateur de politiques d'automatisation :

1. Sélectionnez l'onglet Administration, accédez à Connaissances, Politiques d'automatisation, Planification.

   Le Planificateur de politiques d'automatisation apparaît.

2. Remplissez les champs suivants :
   - **Dernière mise à jour :** sélectionnez la case à cocher Exécuter le calcul des politiques d'automatisation.
   - **Calendrier** : spécifiez la date et l'heure auxquelles CA SDM effectue le calcul et exécute les politiques.
3. Cliquez sur Enregistrer.

Exécution de la fiche de rapport des connaissances.

La fiche de rapport des connaissances affiche des informations sur la contribution en connaissances de chaque utilisateur et indique quels documents de connaissances sont les plus efficaces. Vous pouvez utiliser ces informations pour améliorer les processus de création des documents de connaissances et les processus de mise en place d'un soutien optimal pour les utilisateurs finals de votre environnement.

Pour exécuter la fiche de rapport des connaissances

1. Cliquez sur l'onglet Administration.
2. Accédez à Connaissances, Fiche de rapport des connaissances.

   La carte de rapport des connaissances s'affiche.
3. Complétez les champs suivants, puis cliquez sur Enregistrer :
   - **Dernière mise à jour :** sélectionnez la case à cocher Exécuter le calcul.
   - **Calendrier** : spécifiez la date et l'heure auxquelles CA SDM effectue le calcul et exécute la fiche de rapport.

Remarque : Pour plus d'informations sur l'utilisation des politiques d'automatisation et de la fiche de rapport des connaissances, reportez-vous au *Manuel d'administration*.

Importation d'exemples de données Gestion des connaissances

Des exemples de données Knowledge issues de Knowledge Broker et des accélérateurs Knowledge sont mises à votre disposition. Pour exploiter ces données, vous devez les importer dans la base de données Gestion des connaissances.

Remarque : Les exemples de fichiers ne sont pas localisés. L'importation des données d'exemple ne fonctionne pas sur les environnements localisés.

Pour la disponibilité avancée, exécutez ImportSampleData.bat ou ImportSampleData.sh à partir du serveur d'arrière-plan.

Installation sous Windows

1. Accédez au répertoire $NX_ROOT\samples\data et décompressez le fichier SampleData.zip dans ce même répertoire.
2. Depuis la fenêtre de commande, accédez au registre $NX_ROOT/bin et exécutez le fichier ImportSampleData.bat.

Installation sous UNIX

1. Exécutez la commande tar -xvf SampleData.tar à partir de $NX_ROOT\samples\data.
2. Depuis la fenêtre de commande, accédez au registre $NX_ROOT/bin et exécutez le fichier ImportSampleData.sh.

Configuration du moteur de recherche

Par défaut, le moteur de recherche EBR est installé avec CA SDM.

Remarque : Pour de plus amples renseignements sur les options du moteur de recherche, reportez-vous à l'*Aide en ligne*.

pdm_k_reindex : utilitaire de réindexation des connaissances

L'utilitaire de réindexation des connaissances (pdm_k_reindex.exe) se trouve dans le répertoire d'installation de Gestion des connaissances.

Remarque : La réindexation de documents dans la base de connaissances peut prendre du temps en fonction de la taille de votre base de données. Il est donc recommandé d'exécuter l'utilitaire de réindexation après avoir apporté tous les changements. Dans le cadre d'une configuration de disponibilité avancée, vous ne pouvez pas exécuter l'utilitaire de réindexation des connaissances pendant le basculement.

Important : Sous UNIX, la valeur LIBPATH doit être définie avant d'exécuter plusieurs utilitaires CA SDM. Utilisez pdm_task pour définir la valeur LIBPATH avant l'exécution d'un utilitaire. Par exemple, entrez "pdm_task pdm_clean_attachments ...".

1. Ouvrez l'invite de commande.
2. Entrez la commande suivante dans l'invite de commande pour exécuter la réindexation des connaissances :

Par exemple :

```
pdm_k_reindex
```

Les options suivantes sont disponibles avec cette commande :

-D

Définit le mode de débogage, par exemple, impression dans une fenêtre de commande.

-v

Définit le mode commentaires (par exemple, impression dans le fichier stdlog).

-i

Après la réindexation, ne crée pas d'index de table dans la table de réindexation.

Remarque : Les paramètres comportant un tiret en tant que préfixe, par exemple –D, doivent précéder les autres paramètres ne comportant pas de préfixe.

L'autre option est la suivante :

***fichier*:reindex.txt**

Les documents sont réindexés dans le fichier spécifié.

+i

Une fois la réindexation effectuée, crée les index uniquement de la table réindexée, à savoir la table de recherche. Les index antérieurs sont ignorés avant la réindexation.

+t

Intervertit uniquement les noms des tables de recherche et de réindexation.

Remarque : Un préfixe "+" indique que seul ce paramètre s'applique.

sdtout

Définit la fréquence de la statistique apparaissant dans la fenêtre de commande. Par défaut, l'utilitaire de réindexation des connaissances fournit des statistiques dans la fenêtre de commande tous les 1 000 documents traités. Cependant, il est quelquefois nécessaire que les statistiques soient fournies plus souvent. Utilisez le paramètre suivant :

```
pdm_k_reindex -i sdtout:10
```

Dans ce cas de figure, les statistiques s'affichent dans la fenêtre de commande pour chaque groupe de dix documents.

Les documents sont réindexés dans la base de connaissances.

Nouvelles balises pour configurer un serveur de domaine pour le robot d'indexation de surface

Si CA SDM a un grand nombre de données à indexer, vous devez avoir un serveur dédié au robot d'indexation de surface dans votre configuration CA SDM pour minimiser les effets de ce dernier sur l'environnement CA SDM global :

- Conventionnelle : serveur principal ou secondaire
- Disponibilité avancée : serveur d'applications

  Pour de plus amples renseignements sur la façon de configurer le serveur CA SDM, consultez l'*Aide en ligne de l'utilitaire de configuration du serveur*.

Les balises suivantes sont ajoutées dans le fichier crawler_surface_config.xml pour effectuer l'indexation :

- Une nouvelle balise a été ajoutée au fichier crawler_surface_config.xml root\general_configuration\sdm_domsrvr_name pour permettre au client d'ajouter le nom d'une instance domserver dédiée au robot d'indexation de surface.

  Valeur par défaut : domsrvr

  Cette valeur est un nom d'instance domserver (gestionnaire d'objet) par défaut.
- Une autre balise *sharepoint_properties_file* a également été ajoutée dans le fichier crawler_surface_config.xml, section *root\general_configuration*, afin de permettre au client de le modifier et d'en supprimer le contenu si le robot d'indexation de surface n'est pas utilisé dans SharePoint pour indexer les données CA SDM.

  Valeur par défaut : sharepoint

  Cette valeur est le nom du fichier *sharepoint.properties* disponible par défaut dans NX_ROOT\CATALINA_BASE_FS\lib.

Configuration de CA Workflow

Pour configurer CA Workflow pour l'utiliser avec votre installation CA SDM, effectuez les tâches décrites dans cette section.

Renseignements supplémentaires :

Démarrage et arrêt de CA Workflow (page 278)
Configuration de la connexion automatique (Authentification externe) (page 282)
Configuration de la liste de travail et du gestionnaire de flux de travaux pour la connexion automatique (page 283)
Configuration de CA Workflow Design Environment pour la connexion automatique (page 284)
Options CA Workflow (page 285)
Configuration de l'exemple de flux de travail de gestion des problèmes (page 286)
Configuration du flux de travaux de commande de PC (page 288)
Modifier la définition de processus de gestion des changements - Exemple (page 290)

Démarrage et arrêt de CA Workflow

Vous devez installer et configurer CA SDM avant de pouvoir installer CA Workflow. Le Tomcat de CA SDM par défaut est automatiquement configuré, démarré et arrêté par le gestionnaire de démons de CA SDM. L'utilitaire de ligne de commande pdm_tomcat_nxd peut aussi être utilisé pour démarrer et arrêter l'instance de Tomcat.

1. (Applicable uniquement à la configuration conventionnelle) Configure des processus spécifiques devant être démarrés sur le serveur secondaire.
   a. Exécutez pdm_edit (sur le serveur principal).
   b. Redémarrez les services CA SDM.

      Ce redémarrage permettra de contrôler la version des variables d'environnement spécifiques sur un serveur secondaire, des variables nécessaires pour installer et exécuter CA Workflow

2. Installez et configurez CA Workflow sur le serveur suivant, selon votre configuration de CA SDM :
   - Conventionnelle : serveur principal ou secondaire
   - Disponibilité avancée : l'un des serveurs d'applications
3. Exécutez pdm_tomcat_nxd -d start -t CAWF

   CA Workflow est alors lancé manuellement.

   Remarque : Exécutez *pdm_tomcat_nxd -d stop -t CAWF* pour arrêter CA Workflow.
4. Installez les options de CA Workflow sur le serveur suivant, selon votre configuration de CA SDM :
   - Conventionnelle : serveur principal
   - Disponibilité avancée : serveur d'arrière-plan

   Cela permet à CA Workflow de démarrer et de s'arrêter automatiquement, et d'autoriser les communications entre CA SDM et CA Workflow.

Renseignements supplémentaires :

pdm_tomcat_nxd:Démarrage ou arrêt d'une instance Tomcat (page 279)

pdm_tomcat_nxd:Démarrage ou arrêt d'une instance Tomcat

L'utilitaire *pdm_tomcat_nxd* s'exécute comme un processus démon et comme un utilitaire de ligne de commande. L'utilitaire peut réaliser les opérations suivantes :

- Il traite les demandes à partir de l'utilitaire de ligne de commande pour DEMARRER et ARRETER une instance Tomcat spécifique.
- Il renvoie l'état de Tomcat.
- Il QUITTE le démon et arrête l'instance Tomcat.

Le démon traite aussi les demandes d'un servlet d'"écouteur" Tomcat pour mettre à jour l'état de l'instance Tomcat lorsqu'elle est arrêtée ou démarrée.

L'utilitaire de ligne de commande pdm_tomcat_nxd dirige les requêtes DEMARRAGE, ARRET, ETAT et QUITTER vers un démon Tomcat ou peut directement DEMARRER ou ARRETER une instance Tomcat spécifique, sans utiliser de démon Tomcat.

Pdm_tomcat_nxd fournit plusieurs démons qui sont démarrés sur un seul serveur CA SDM, chaque démon maintenant une instance Tomcat spécifique. Chaque démon est initialisé avec un Tomcat et un nom de serveur spécifiques qui sont utilisés pour composer l'adresse slump du démon, l'adresse slump de son "écouteur" et le répertoire Catalina Base où l'instance Tomcat est définie. Cette modification est prise en charge par un nouveau paramètre de nom Tomcat.

Utilisez la commande suivante pour démarrer un démon pdm_tomcat_nxd. Quand le démon démarre, il démarre automatiquement une instance Tomcat avec un nom Tomcat spécifié.

Remarque : Dans les exemples suivants, le nom Tomcat par défaut est vide (sous-entendu "ServiceDesk").

```
pdm_tomcat_nxd -s [ -t tomcat ]
```

Exemple : Envoyez une demande à un démon Tomcat spécifique sur un serveur spécifique

Si la demande est ETAT, un message est d'abord envoyé à l'"écouteur" Tomcat. S'il n'y a pas de réponse, la demande est alors envoyée au démon Tomcat. Le nom de serveur par défaut est NX_LOCAL_HOST. Le nom Tomcat par défaut est vide ; (ce qui sous-entend "ServiceDesk").

```
pdm_tomcat_nxd -c <request> [-t <tomcat_name> ] [-S <server_name> ]
```

Demande

ARRETER | ARRET | DEMARRER | ETAT | QUITTER |

Exemple : Démarrez ou arrêtez un Tomcat spécifique sur ce serveur (sans utiliser le démon Tomcat)

```
pdm_tomcat_nxd -d <request> [ -t <tomcat_name> ]
```

Demande

ARRETER | DEMARRER

Exemple : Affichez la commande Tomcat qui sera utilisée pour démarrer et arrêter une instance Tomcat

```
pdm_tomcat_nxd -T [ -t <tomcat_name> ]
```

Quand le processus du démon commence, il se connecte au serveur slump à l'aide d'un nom de processus composé de server_name et du nom du Tomcat (s'il est spécifié). L'utilitaire de ligne de commande utilise cette adresse pour envoyer des messages au démon. Pour envoyer des demandes ETAT à l'"écouteur" de Tomcat, l'utilitaire de ligne de commande utilise le nom de processus de l'écouteur composé aussi de server_name et de tomcat_name (s'il est spécifié). Le démon ouvre aussi un fichier journal pour l'instance Tomcat à l'aide d'un nom de fichier journal composé du nom du Tomcat (s'il est spécifié). Les exemples suivants présentent les variables daemon_name, listener_name et nom de fichier de journal :

```
daemon_name
    "pdm_tomcat -" +
    server_name
    [ + "-" + tomcat_name ] si tomcat_name est spécifié

listener_name = server_name + "-" +
    "container-pdmContextListener"
    [ +  "-" + tomcat_name ] si tomcat_name est spécifié

tomcat_log = pdm_tomcat +
     "-" + tomcat_name + ] si tomcat_name est spécifié
    .log
```

Quand l'utilitaire de ligne de commande ou le processus de démon démarre ou arrête une instance Tomcat, une commande (catalina_cmd) est générée à l'aide de diverses variables d'environnement NX. Toutes les variables d'environnement suivantes sont requises, sauf NX_JAVA_OPTIONS et NX_TOMCAT_HOTSPOT qui est uniquement utilisée sur un système HP.

Les variables d'environnement (pour l'instance Tomcat de ServiceDesk par défaut) n'incluent pas de nom Tomcat dans leur nom. En revanche, les variables d'environnement de toutes les autres instances Tomcat peuvent facultativement utiliser un nom Tomcat dans leur nom de variable, sauf NX_XXX_CATALINA_BASE où le nom Tomcat (XXX) doit être spécifié. Si une variable d'environnement spécifique de Tomcat n'existe pas, le nom de variable d'environnement par défaut est utilisé.

```
CATALINA_BASE  | NX_XXX_CATALINA_BASE
NX_TOMCAT_INSTALL_DIR + [ _XXX ]
NX_TOMCAT_INSTALL_DIR + [ _XXX ]
NX_JRE_INSTALL_DIR + [ _XXX ]
NX_JDBC_DRIVER + [ _XXX ]
NX_JAVA_OPTIONS + [ _XXX ]
NX_JDBC_DRIVER_CLASSPATH + [ _XXX ]
NX_TOMCAT_HOTSPOT + [ _XXX ]
```

Configuration de la connexion automatique (Authentification externe)

Pour automatiser le processus de connexion pour les tâches de la liste de travail de CA Workflow lors de l'utilisation des demandes de changement, des demandes, des incidents, des problèmes et des demandes client, vous pouvez configurer la connexion automatique. L'utilisation de la connexion automatique vous évite de devoir entrer un ID utilisateur et un mot de passe lorsque vous cliquez sur le lien d'une liste de travail. La connexion automatique utilise vos informations d'identification de domaine du système d'exploitation Windows pour vous connecter à la liste de travail.

Remarque : Pour que la connexion automatique fonctionne correctement, il n'est *pas* nécessaire d'inclure l'utilisateur dans les groupes Administrateurs de flux de travaux, Initiateurs des processus de flux de travaux ou Superutilisateur Workflow dans CA EEM. Ces groupes fournissent des niveaux d'accès différents aux utilisateurs connectés à CA Workflow Design Environment.

Pour configurer la connexion automatique pour les tâches de la liste de travail (Windows uniquement)

1. Installez et configurez CA Workflow (page 228).
2. Configurez la liste de travail et le gestionnaire de flux de travaux pour la connexion automatique (page 283).
3. Configurez CA EEM pour qu'il référence un répertoire externe (par exemple, Microsoft Active Directory) pour authentifier les utilisateurs. Pour obtenir des informations, reportez-vous à la documentation relative à CA EEM.

   Remarque : L'utilisateur doit disposer d'un enregistrement d'utilisateur CA EEM et de l'enregistrement de contact CA SDM correspondant valide pour le même compte d'utilisateur, pour pouvoir accéder à la liste de travail et pour que la connexion automatique fonctionne correctement. Parce qu'un élément apparaisse dans la liste de travail et pour profiter des groupes Administrateurs de flux de travaux, Initiateurs des processus de flux de travaux ou Superutilisateur Workflow dans CA EEM, un enregistrement d'utilisateur de CA EEM valide est nécessaire.
4. Connectez-vous à CA SDM.
5. Cliquez sur l'onglet Administration.
6. Dans l'arborescence à gauche, cliquez sur Gestionnaire d'options, CA Workflow.

   La liste des options s'affiche.

7. Vérifiez que le nom de l'utilisateur de cawf_username et le mot de passe de cawf_password correspond à un utilisateur valide dans le domaine défini dans CA EEM. Si ce n'est pas le cas, utilisez CA EEM pour ajouter l'utilisateur au domaine.

   Important : Dans le gestionnaire d'options, les valeurs de cawf_username et de cawf_password sont définies en fonction des valeurs spécifiées pour le nom et le mot de passe de l'utilisateur privilégié lors de la configuration de CA SDM après l'installation. Si l'utilisateur privilégié spécifié pendant la configuration de CA SDM n'est pas disponible lorsque CA EEM est configuré pour référencer le répertoire externe, la connexion automatique ne fonctionnera *pas*. Dans ce cas, utilisez CA EEM pour ajouter l'utilisateur au domaine ou modifiez les informations de cawf_username et de cawf_password pour inclure un utilisateur de domaine valide configuré dans CA EEM.

8. Connectez-vous à CA SDM et créez une demande de changement, une demande, un incident, un problème ou une demande client avec la catégorie appropriée.

   Remarque : Vérifiez que la catégorie est configurée pour utiliser CA Workflow et comporte une définition CA Workflow liée à l'application avant de créer la demande de changement, la demande, l'incident, le problème ou la demande client.

   Vous pourrez à présent cliquer sur un lien dans la liste de travail et vous connecter sans devoir entrer un ID utilisateur et un mot de passe.

Informations complémentaires :

Configuration de CA Workflow Design Environment pour la connexion automatique (page 284)

Configuration de la liste de travail et du gestionnaire de flux de travaux pour la connexion automatique

Vous pouvez activer la connexion automatique pour la liste de travail et le gestionnaire de flux de travaux en définissant la valeur de la variable *automaticLoginEnabled* sur true (vrai) dans les fichiers web.xml de la liste de travail et du gestionnaire de flux de travaux (wl.xml et pm.xml). Les entrées sont les mêmes dans les deux fichiers web.xml.

```
<env-entry>
    <env-entry-name>automaticLoginEnabled</env-entry-name>
    <env-entry-value>true</env-entry-value>
    <env-entry-type>java.lang.Boolean</env-entry-type>
<env-entry>
```

La valeur initiale de la liste de travail et du gestionnaire de flux de travaux est définie pendant l'installation en fonction du paramètre du fichier de réponse.

```
# Activer ou désactiver la connexion automatique (appelé aussi Signature unique)

-P serverAction.automaticLoginEnabled="true"
```

Pour configurer la liste de travail et le gestionnaire de flux de travaux pour la connexion automatique.

1. Recherchez les fichiers pm.xml et wl.xml dans le répertoire suivant :

   $NX_ROOT\bopcfg\www\CATALINA_BASE_WF\conf\Catalina\localhost

2. Modifiez pm.xml et wl.xml, ainsi que la valeur de la ligne suivante :

   - (Avant modification) <Environment name="automaticLoginEnabled" override="true" type="java.lang.Boolean" value="*false*"/>
   - (Après modification) <Environment name="automaticLoginEnabled" override="true" type="java.lang.Boolean" value="*true*"/>

3. Arrêtez le serveur Tomcat à l'aide de la commande suivante :

   ```
   pdm_tomcat_nxd -d STOP -t CAWF
   ```

4. Démarrez le serveur Tomcat pour recréer ces deux dossiers à l'aide de la commande suivante :

   ```
   pdm_tomcat_nxd -d START -t CAWF
   ```

5. Accédez à un ticket avec une tâche de flux de travaux et sélectionnez l'une des tâches.

6. La liste de travail apparaît et la connexion automatique réussit.

Remarque : Si vous reconfigurez CA Workflow et que vous référencez un serveur CA EEM différent, vous devez fermer le Tomcat de CA Workflow, supprimer les dossiers *pm* et *wl* qui se trouvent dans *$NX_ROOT\bopcfg\www\CATALINA_BASE_WF\webapps*, puis redémarrer le Tomcat de CA Workflow pour que ces dossiers soient recréés avec les nouvelles informations du serveur CA EEM.

Configuration de CA Workflow Design Environment pour la connexion automatique

La connexion automatique pour CA Workflow Design Environment est activée à l'aide du paramètre de ligne de commande *-auto*.

Options CA Workflow

Les options suivantes contrôlent la fonctionnalité CA Workflow.

Important : Après l'installation de CA Workflow et CA EEM, vous devez définir manuellement certaines options, comme le numéro de port, dans le Gestionnaire d'options. Par exemple, une application Web Tomcat différente est utilisée pour CA Workflow donc elle ne peut plus utiliser le port par défaut 8080. Pour éviter tout conflit de port, la valeur par défaut 8090 est utilisée. Pour plus d'informations, reportez-vous au *Manuel de mise en oeuvre*.

cawf_hostname

Indique le nom d'hôte du serveur sur lequel CA Workflow est installé. Définissez cette variable uniquement si CA Workflow est installé à partir du média de CA SDM ; sinon, n'installez pas cette option.

cawf_password

Indique le mot de passe de l'utilisateur IDE CA Workflow. Pendant l'installation de CA Workflow, l'Assistant d'installation des composants de CA SDM utilise la valeur du Mot de passe d'utilisateur de flux de travaux pour définir le cawf_password.

cawf_pm_location

Indique l'emplacement de l'application Gestionnaire de processus CA Workflow. L'URL doit suivre le format suivant :
`http://<wf_hostname>:8090/pm`

cawf_pm_url

Indique l'URL du service Web du Gestionnaire de processus CA Workflow. L'URL doit suivre le format suivant :
`http://<wf_hostname>:8090/pm/services/pmService2`

cawf_username

Indique le nom d'utilisateur CA Workflow de l'utilisateur IDE CA Workflow. Pendant l'installation de CA Workflow, l'Assistant d'installation des composants de CA SDM utilise la valeur du Nom d'utilisateur de flux de travaux pour définir le cawf_username.

cawf_wl_location

Indique l'emplacement de l'application Gestionnaire de listes de travail CA Workflow. L'URL doit suivre le format suivant :
`http://<wf_hostname>:8090/wl`

cawf_wl_url

Indique l'URL du service Web de listes de travail CA Workflow. L'URL doit suivre le format suivant :
`http://<wf_hostname>:8090/wl/services/wlService`

Important : L'installation ou la désinstallation d'une option requiert le redémarrage des serveurs CA SDM. Pour la configuration de disponibilité avancée, toutes les options ne requièrent pas le redémarrage de tous les serveurs. Avant de redémarrer un serveur, lisez la Liste de redémarrage des serveurs.

Configuration de l'exemple de flux de travail de gestion des problèmes

L'exemple de flux de travaux de gestion des problèmes guide la décision de créer ou non une demande de changement pour un ticket de problème particulier. Une fois que le destinataire d'un problème a effectué des recherches, il effectue une enquête sur le problème pour créer une recommandation. L'enquête donne à l'approbateur une idée de l'impact du problème et indique s'il est nécessaire de le résoudre par la gestion des changements. Le concept sous-jacent de ce flux de travaux (gravité du problème/analyse de valeur) est dérivé d'ITIL v3.

Remarque : Pour plus d'informations sur l'exécution des tâches CA SDM dans le processus suivant, consultez l'*Aide en ligne*.

Pour configurer l'exemple de flux de travail Gestion des problèmes :

1. Créez un contact de CA SDM pour un analyste (par exemple, l'analyste Jeanne) en utilisant les valeurs suivantes :

   Type de contact

   Sélectionnez Analyste.

   Partition de données

   Sélectionnez Analyste du centre de services.

   Type d’accès

   Sélectionnez Personnel du centre de services.

Adresse de courriel

Entrez une adresse de courriel.

Remarque : A des fins de test, vous pouvez entrer votre propre adresse de courriel.

Méthode de notifications

Sélectionnez un courriel pour les notifications Basses, Normales, Hautes et Urgence.

2. Créez un contact de CA SDM pour un superviseur (par exemple, le superviseur Jean) en utilisant les valeurs suivantes :

Type de contact

Sélectionnez Gestionnaire.

Partition de données

Sélectionnez Personnel du centre de services.

Type d'accès

Sélectionnez Personnel du centre de services.

Adresse de courriel

Entrez une adresse de courriel.

Remarque : A des fins de test, vous pouvez entrer votre propre adresse de courriel.

Méthode de notifications

Sélectionnez un courriel pour les notifications Basses, Normales, Hautes et Urgence.

3. Créez un enregistrement d'utilisateur EEM associé pour les contacts de CA SDM de l'analyste Jeanne et du superviseur Jean.

   Remarque : Les ID utilisateur des enregistrements EEM doivent corresondre à ceux des enregistrements de contact. Pour plus d'informations sur la création d'enregistrements utilisateur EEM, reportez-vous à l'*Aide en ligne de EEM*.

4. Affectez Jean comme superviseur sur l'enregistrement de contact de l'analyste Jeanne.

5. Créez un CI (par exemple, Serveur Exchange).

6. Créez un code de cause première (par exemple, mise à niveau de RAM requis).

7. Créez un domaine de problème (par exemple, ProblemMgmt.SampleWF).

8. Associez le domaine de problème ProblemMgmt.SampleWF avec l'exemple de flux de travaux Gestion des problèmes.

9. Créez un ticket de problème avec les attributs suivants :

   Catégorie de problème

   Sélectionnez ProblemMgmt SampleWF.

   Elément de configuration

   Sélectionnez Serveur Exchange.

   Destinataire

   Sélectionnez Analyste, Jeanne.

10. Connectez-vous à CA SDM en tant que Jeanne, Analyste et testez la configuration de flux de travaux.

    Remarque : Vous devez effectuer la recherche de problème avant de remplir le premier formulaire du flux de travaux. Pour plus d'informations sur la rélisation des tâches de flux de travaux, consultez l'*Aide en ligne de CA Workflow*.

Configuration du flux de travaux de commande de PC

L'exemple de flux de travaux de commande de PC guide le processus de gestion des changements pour la commande d'un nouveau PC.

Remarque : Pour plus d'informations sur la réalisation de chacune des tâches CA SDM dans le processus suivant, reportez-vous à l'*Aide en ligne*.

Pour configurer et tester l'exemple de flux de travaux de commande de PC :

1. Créez un contact de CA SDM pour un employé (par exemple, l'employé Guillaume) en utilisant les valeurs suivantes :

   Type de contact

   Sélectionnez Employé.

   Partition de données

   Sélectionnez Employé.

   Type d’accès

   Sélectionnez Employé.

Adresse de courriel

Entrez une adresse de courriel.

Remarque : A des fins de test, vous pouvez entrer votre propre adresse de courriel.

Méthode de notifications

Sélectionnez un courriel pour les notifications Basses, Normales, Hautes et Urgence.

2. Créez un contact de CA SDM pour un analyste (par exemple, l'analyste Jeanne) en utilisant les valeurs suivantes :

Type de contact

Sélectionnez Analyste.

Partition de données

Sélectionnez Analyste du centre de services.

Type d'accès

Sélectionnez Personnel du centre de services.

Adresse de courriel

Entrez une adresse de courriel.

Remarque : A des fins de test, vous pouvez entrer votre propre adresse de courriel.

Méthode de notifications

Sélectionnez un courriel pour les notifications Basses, Normales, Hautes et Urgence.

3. Créez un enregistrement d'utilisateur EEM associé pour les contacts CA SDM de l'employé Guillaume et de l'analyste Jeanne.

Remarque : Les ID utilisateur des enregistrements EEM doivent corresondre à ceux des enregistrements de contact. Pour plus d'informations sur la création d'enregistrements utilisateur EEM, reportez-vous à l'*Aide en ligne de EEM*.

4. Créez une catégorie de changement (par exemple, Commande.PC).
5. Affectez l'analyste Jeanne comme destinataire de la catégorie de changement.
6. Créez un ticket de demande de changement avec les attributs suivants :

Catégorie de changement

Sélectionnez Commande.PC.

Destinataire

Sélectionnez Analyste, Jeanne.

7. Connectez-vous à CA SDM en tant que Jeanne, Analyste et testez la configuration de flux de travaux.

   Remarque : Pour plus d'informations sur la réalisation des tâches de flux de travaux, reportez-vous à l'*Aide en ligne de CA Workflow*.

Modifier la définition de processus de gestion des changements - Exemple

Cet exemple montre comment la définition de processus de gestion des changements gère les demandes de changement en utilisant les directives ITIL v3 suivantes :

- Evaluation des risques
- Analyse d'impact et de conflits
- Approbations par le gestionnaire de changements et le CAB
- Analyse et évaluation de la mise en oeuvre

Remarque : Cet exemple suppose que CA SDM utilise CA Workflow et que la définition de processus de gestion des changements est configurée. Pour plus d'informations sur la configuration de la définition de processus de gestion des changements, reportez-vous au *Manuel d'administration*.

Exemple de préparation d'une demande de changement pour approbation

Cet exemple configure une catégorie de changement et prépare une demande de changement pour approbation. En tant qu'administrateur, vous configurez la catégorie de changement pour utiliser la définition de processus de gestion des changements et définissez les groupes et les contacts. En tant que demandeur, vous réalisez une enquête d'évaluation des risques, effectuez l'analyse d'impact et de conflit et, enfin, effectuez l'analyse des changements.

Remarque : Pour plus d'informations sur la configuration de la catégorie de changement et sur l'utilisation de la définition de processus de gestion des changements, reportez-vous à l'*Aide en ligne* et au *Manuel d'administration*.

Pour préparer une demande de changement pour approbation, procédez comme suit :

1. Connectez-vous comme administrateur et créez ou modifiez une catégorie de changement à l'aide des options suivantes, puis cliquez sur Utiliser CA Workflow :
   - **CAB** : sélectionnez le groupe de CAB.
   - **Groupe** : spécifiez le groupe de mise en oeuvre.
   - **Examen du risque** : sélectionnez Général.
   - **Nom de la définition de CA Workflow** : sélectionnez Change Mgmt - Service Desk r12.1 (sous l'onglet Flux de travaux).

2. Créez les ID utilisateur et les contacts CA SDM suivants, puis affectez-les à leurs groupes respectifs dans CA SDM et CA EEM :
   - **Don Requester** : contact qui crée la demande de changement.
   - **John Approver** : gestionnaire du groupe de mise en oeuvre qui agit comme le gestionnaire de changements pour approuver une demande de changement. Un gestionnaire du groupe de CAB qui agit comme approbateur de CAB.
   - **Sue Implementer** : membre du groupe de mise en oeuvre qui exécute également les éléments de travail de demande de changement.
3. Connectez-vous sous le nom Don Requester et créez une demande de changement avec les valeurs suivantes :
   - **Demandeur** : indiquez Don Requester.
   - **Catégorie** : indiquez la catégorie de changement à l'aide de la définition de processus de gestion de changements.
   - **Type** : sélectionnez Normal.
   - **Résumé de la demande/Description de la demande** : indiquez la raison de la demande de changement.
   - **Date planifiée de début** : spécifiez une date de début.
   - **Durée planifiée** : indiquez la durée.
   - **CI** : indiquez les CI concernés (onglet Eléments de configuration).

   Don Requester reçoit une notification par courriel pour terminer l'enquête d'évaluation des risques. La page Détail de la demande de changement affiche l'état Demande de changement.
4. Cliquez sur Enquête sur les risques, puis répondez aux questions de l'enquête d'évaluation des risques pour que la demande de changement soit classée en risque élevé. Cliquez sur Soumettre et Confirmer.

   Le système génère une valeur de risque pour la demande de changement et le demandeur reçoit une notification par courriel pour commencer l'analyse d'impact et de conflit.

   Remarque : Vous pouvez uniquement passer à la tâche suivante après avoir cliqué sur Confirmer dans la page Effectuer la tâche.
5. Sous l'onglet de Tâches de flux de travaux, suivez les liens pour accéder à l'onglet Conflits des demandes de changement.
6. Cliquez sur Analyse du conflit pour examiner et résoudre tous les conflits de planification des CI.
7. Sous l'onglet Eléments de configuration, cliquez sur Analyse d'impact pour examiner les informations sur chaque CI.
8. Sous l'onglet Eléments de configuration, cliquez sur l'explorateur d'impact et accédez à l'onglet Relations CA CMDB pour prendre en compte l'impact de la demande de changement sur les CI associés.

9. Accédez à la page Effectuer la tâche, puis cliquez sur Confirmer.

   Don Requester reçoit une notification par courriel pour effectuer l'analyse des changements.

10. Sous l'onglet Tâches de flux de travaux, suivez les liens pour accéder à l'onglet Analyse des changements de la demande de changement. Répondez aux questions pour confirmer la demande de changement et cliquez sur Soumettre.

    John Approver reçoit une notification par courriel pour approuver la demande de changement. La page Détail de la demande de changement affiche les éléments suivants : Etat : Approbation en cours.

    - Approbation du CAB : Oui

Exemple d'approbation et de mise en oeuvre d'une demande de changement

Cet exemple affiche les tâches d'approbation et de mise en oeuvre à effectuer tout en utilisant la définition de processus de gestion des changements pour gérer les demandes de changement. Comme approbateur, vous examinez les informations d'analyse des changements et approuvez la demande de changement. Comme membre du groupe de mise en oeuvre, vous effectuez le travail affecté sur la demande de changement et menez une analyse post-mise en oeuvre qui décrit le résultat de la demande de changement.

Remarque : Pour plus d'informations sur l'utilisation de la définition de processus de gestion des changements, reportez-vous au *Manuel d'administration*.

Pour approuver et exécuter la demande de changement, procédez comme suit :

1. Connectez-vous sous le nom John Approver et ouvrez la demande de changement.
2. Sous l'onglet Tâches de flux de travaux, suivez les liens pour accéder à l'onglet Approbation du gestionnaire de changements, puis cliquez sur Approuver.

   Comme la demande de changement est classée en risque élevé, l'état est Approbation en cours. Etant donné que cet exemple utilise également John Approver comme membre du groupe de CAB, John Approver reçoit une notification par courriel pour examiner la demande de changement comme membre du CAB.

3. Sous l'onglet Approbation du CAB, cliquez sur Approuver.

   La page Détail de la demande de changement affiche l'état Approuvé. Sue Implementer reçoit une notification par courriel.

4. Connectez-vous sous le nom de Sue Implementer, puis ouvrez la demande de changement.

5. Sous l'onglet Tâches de flux de travaux, accédez à la page Effectuer des tâches, puis cliquez sur Confirmer.

   La page Détail de la demande de changement affiche l'état Mise en oeuvre en cours.

6. Sous l'onglet Tâches de flux de travaux, suivez les liens pour accéder à l'onglet Mise en oeuvre terminée.

7. Répondez aux questions pour décrire l'évolution de la demande de changement, puis cliquez sur Terminé.

   La demande de changement est clôturée. La page Détail de la demande de changement affiche l'état Mis en oeuvre et le Code de clôture Terminé. Sue Implementer reçoit une notification par courriel pour effectuer le PIR.

8. Sous l'onglet Tâches de flux de travaux, suivez les liens pour accéder à l'onglet PIR.

9. Sous l'onglet PIR, répondez aux questions pour décrire la résolution et cliquez sur Soumettre.

   La demande de changement est clôturée. La page Détail de la demande de changement affiche l'état Clôturé. L'onglet Tâches de flux de travaux affiche le lien Clôturer la demande de changement avec des informations supplémentaires. L'onglet Activités de demande de changement affiche l'état final de la définition de processus de gestion des changements.

Configuration de l'intégration des flux de travaux CA Process Automation

Pour configurer l'intégration des flux de travaux CA Process Automation, procédez de la manière suivante :

1. Assurez-vous que CA Process Automation et CA SDM fonctionnent comme des entités autonomes.

   Important : Si CA Process Automation est configuré en mode FIPS, vous devez également configurer le serveur EEM et le SDK d'EEM en mode FIPS. Pour de plus amples renseignements sur la configuration du SDK d'EEM en mode FIPS, consultez la documentation de CA EEM.

2. Configurez les options des flux de travaux CA Process Automation.

3. Créez les groupes et ID d'utilisateurs nécessaires pour accorder l'accès approprié à CA Process Automation aux utilisateurs de CA SDM .

Renseignements supplémentaires :

Vérifier les installations de CA Process Automation et de CA SDM (page 294)
Configurer les options de flux de travaux de CA Process Automation (page 294)
Administration utilisateur de CA Process Automation (page 298)
Prise en charge de l'authentification unique de CA SDM vers CA Process Automation en utilisant CA EEM (page 299)

Vérifier les installations de CA Process Automation et de CA SDM

Vous pouvez intégrer CA Process Automation et CA SDM de façon à ce qu'ils coexistent sur un même serveur lorsque l'architecture du serveur prend en charge ces deux produits. Quand les composants de CA Process Automation ou de CA SDM ne peuvent pas s'intégrer sur le même serveur, vous devez envisager d'installer ces produits sur des serveurs séparés.

Avant de configurer CA Process Automation et CA SDM, vous pouvez confirmer que les deux produits sont installés et fonctionnent de façon indépendante.

Remarque : Pour plus d'informations sur les exigences des produits CA SDM et CA Process Automation, reportez-vous aux *Notes de parution* de CA SDM.

Pour vérifier les installations de CA Process Automation et de CA SDM

1. Ouvrez un navigateur sur le serveur qui héberge CA SDM et vérifiez qu'un utilisateur de CA Process Automation peut se connecter à CA Process Automation. Modifiez les espaces réservés pour correspondre à l'installation CA Process Automation cible.
   `http(s)://<server>:CA Portal/itpam`
2. Entrez l'URL suivante : Modifiez les espaces réservés pour correspondre à l'installation CA Process Automation cible.
   `http(s)://<server>:CA Portal/itpam/JNLPRequestProcessor?processType=startUI`

   Le produit CA Process Automation est accessible à partir de l'hôte CA SDM.

Configurer les options de flux de travaux de CA Process Automation

Quand vous configurez des options de flux de travaux de CA Process Automation, vous spécifiez la connectivité entre CA SDM et CA Process Automation. Si vous utilisez CA EEM pour l'authentification, vous spécifiez aussi le nom d'hôte de CA EEM.

Pour configurer les options de flux de travaux de CA Process Automation

1. Dans l'onglet Administration, sélectionnez Gestionnaire d'options, Flux de travaux de CA IT PAM.

   La liste des options s'affiche.

2. Cliquez avec le bouton droit de la souris sur chaque option et dans le menu contextuel, sélectionnez Modifier. Configurez les options suivantes :

   caextwf_eem_hostname

   Spécifie le nom du serveur CA EEM. Par exemple, *pam.host.com* identifie l'hôte d'authentification. Vous installez caextwf_eem_hostname uniquement si vous avez configuré CA Process Automation de sorte à utiliser CA EEM en tant que serveur d'authentification. CA SDM utilise cette valeur pour convertir un nom d'utilisateur et un mot de passe en jeton CA EEM. Ainsi, le nom d'utilisateur et le mot de passe ne sont pas transmis en texte simple par l'entremise du protocole HTTP.

   Remarque : si l'installation de CA Process Automation n'utilise pas CA EEM, ne placez pas de valeur dans l'option caextwf_eem_hostname, et n'installez pas caextwf_eem_hostname. La définition d'une valeur fausse ou l'installation de caextwf_eem_hostname quand ce n'est pas nécessaire entraîne l'échec de l'intégration.

   caextwf_endpoint

   Spécifie l'URL pointant vers les services Web de CA Process Automation en incluant le nom d'hôte de CA Process Automation, le port, et le chemin d'accès d'itpam/SOAP obligatoire. Par exemple, http://pam.host.com:pam-Tomcat-port/itpam/soap identifie le terminal. Si la mise en oeuvre utilise CA EEM, l'installation de l'option caextwf_eem_hostname est requise pour le fonctionnement correct de l'intégration entre CA Process Automation et CA SDM.

   caextwf_log_categories

   Spécifie une liste séparée par des virgules de noms de catégorie de journal d'instance de processus de CA Process Automation à afficher dans la demande de changement CA SDM et dans l'onglet Tâches du flux de travaux de demandes client. Par exemple, *Operator,Response,MyOwnCategory* fournit trois catégories de journaux.

   Vous installez caextwf_log_categories selon les décisions opérationnelles du personnel de maquette de processus de CA SDM et CA Process Automation. Cette option ajuste les données par défaut qui apparaissent dans l'onglet de Tâches du flux de travaux pour les demandes, les demandes de changement et les demandes client.

Quand vous installez l'option caextwf_log_categories, tous les messages du journal d'instance de processus de CA Process Automation de la catégorie Processus et des catégories spécifiées apparaissent dans l'onglet Tâches du flux de travaux. Quand vous n'installez pas caextwf_log_categories, seuls les messages du journal d'instance de processus CA Process Automation de la catégorie Processus apparaissent dans l'onglet Tâches du flux de travaux.

Remarque : Pour plus d'informations sur les catégories de messages de journal prédéfinis CA Process Automation, et sur la définition de catégories de messages personnalisés, reportez-vous à la documentation de référence de CA Process Automation.

caextwf_processdisplay_url

Spécifie comment lancer un instantané graphique d'une instance de processus de CA Process Automation en fournissant le nom d'hôte et le chemin d'accès /itpam/JNLPRequestProcessor?processType=startUI&roid path obligatoire. Par exemple, *http://pam.host.com:pam-Tomcat-port//itpam/JNLPRequestProcessor?processType=startUI&roid=* lance un instantané d'une instance de processus. Dans l'onglet Tâches du flux de travaux d'une demande, de la demande de changement ou de la demande client, l'utilisateur sélectionne Afficher le processus pour visualiser l'instantané.

L'installation de l'option caextwf_processdisplay_url est requise pour que l'intégration entre CA Process Automation et CA SDM fonctionne correctement.

caextwf_worklist_url

Spécifie le chemin d'accès d'instance de processus en fournissant le nom d'hôte et le chemin d'accès /itpam?webPage=mytaskfilter&view=tasklist obligatoire. Par exemple, *http://pam.host.com:pam-Tomcat-port/itpam?webPage=mytaskfilter&view=tasklist* permet aux utilisateurs CA SDM d'afficher une liste d'instances de processus CA Process Automation qui doivent faire l'objet d'une attention particulière. La liste apparaît dans CA Process Automation quand l'utilisateur de CA SDM sélectionne un lien associé à une tâche répertoriée dans la demande, la demande de changement ou l'onglet Tâches du flux de travaux de demande client.

L'installation de l'option caextwf_worklist_url est requise pour que l'intégration entre CA Process Automation et CA SDM fonctionne correctement.

caextwf_ws_password

Spécifie le mot de passe administratif associé au nom d'utilisateur de CA Process Automation de l'option caextwf_ws_user. CA SDM utilise le nom d'utilisateur et le mot de passe pour accéder aux fonctions de service Web de CA Process Automation afin d'effectuer des activités d'intégration telles que la sélection de formulaires de demande de démarrage, des informations de définition de processus et des informations d'instance de processus.

L'installation de l'option caextwf_ws_password est requise pour l'intégration entre CA Process Automation et CA SDM. Les mot de passe et nom d'utilisateur spécifiés requièrent l'accès approprié à CA Process Automation. Cependant, il n'est pas nécessaire que le nom de l'utilisateur et le mot de passe de CA Process Automation existent dans les enregistrements de contact de CA SDM.

caextwf_ws_user

Spécifie le nom d'administrateur de CA Process Automation associé au nom d'utilisateur de CA Process Automation de l'option caextwf_ws_password. CA SDM utilise le nom de l'utilisateur et le mot de passe pour accéder aux fonctions de service Web CA Process Automation. Ces services réalisent des activités d'intégration telles que la sélection de formulaires de demande de démarrage, la sélection d'informations de définition de processus, la sélection d'informations sur des instances de processus, ou le lancement d'instances de processus.

L'installation de l'option caextwf_ws_user est requise pour que l'intégration entre CA Process Automation et CA SDM fonctionne correctement. Les nom d'utilisateur et mot de passe spécifiés requièrent l'accès approprié à CA Process Automation. Cependant, il n'est pas nécessaire que le nom de l'utilisateur et le mot de passe de CA Process Automation existent dans les enregistrements de contact de CA SDM.

3. Cliquez sur Installer.
4. Redémarrez le service CA SDM.

   Les produits CA SDM et CA Process Automation peuvent communiquer, même s'il n'existe aucune donnée d'instance de processus. CA SDM et CA Process Automation sont prêts à vous permettre de créer des définitions de processus de CA Process Automation et des formulaires de demande de démarrage de CA Process Automation.

Remarque : Pour plus d'informations sur la création de définitions de processus CA Process Automation et de formulaires de demande de démarrage de CA Process Automation, reportez-vous au *Manuel d'administration* et à la documentation utilisateur de CA Process Automation.

Administration utilisateur de CA Process Automation

CA Process Automation et CA SDM, parce qu'ils sont des produits autonomes, imposent des conditions qui leurs sont particulières en matière d'authentification et d'autorisation. Pour prendre en charge une stratégie d'architecture orientée services (SOA), vous pouvez configurer ces deux produits pour qu'ils utilisent CA EEM pour l'authentification.

Quand vous installez CA Process Automation avec CA EEM comme serveur d'authentification, le programme d'installation crée plusieurs politiques et quatre entités essentielles par défaut :

- Deux utilisateurs d'application : itpamadmin, itpamuser. Pour CA Process Automation 3.1 SP1 : pamadmin et pamuser
- Deux groupes d'applications : ITPAMAdmins, ITPAMUsers. Pour CA Process Automation 3.1 SP1 : PAMAdmins et PAMUsers.

Les utilisateurs CA SDM qui utilisent également CA Process Automation peut être répartis entre ITPAMAdmins (PAMAdmins pour CA Process Automation 3.1 SP1) et ITPAMUsers comme suit :

- Les analystes CA SDM doivent être membres d'ITPAMUsers (PAMUsers pour CA Process Automation 3.1 SP1) lorsque leurs responsabilités englobent les tâches suivantes :
  - l'approbation, le rejet ou tout autre type de réponse aux formulaires de demande d'interaction de CA Process Automation ;
  - le répertoriage des instances de processus CA Process Automation affectées à l'utilisateur ;
  - la consultation de l'affichage graphique en cliquant sur le bouton Afficher le processus sur l'écran d'état de processus de CA Process Automation. Le groupe ITPAMUsers de CA Process Automation (PAMUsers for 3.1 SP1) requiert une politique CA Process Automation supplémentaire pour octroyer l'accès aux graphiques.
- Les analystes CA SDM sont membres d'ITPAMAdmins (PAMAdmins pour 3.1 SP1) lorsque leurs responsabilités englobent les tâches suivantes :
  - la création et la vérification des définitions de processus CA Process Automation ou de formulaires de demande de démarrage ;
  - l'arrêt d'instances de processus directement dans CA Process Automation. L'arrêt d'instances de processus est une exception administrative apportée aux procédures d'intégration attendues ;
  - la délégation des tâches d'instances de processus CA Process Automation ;
  - si l'utilisateur correspond au nom d'utilisateur défini dans le gestionnaire d'options de CA SDM.

- Les utilisateurs de CA SDM ne requièrent pas d'accès à CA Process Automation leurs responsabilités englobent :
  - la création de demandes, de demandes de changement et de problèmes qui lancent des instances de instances ;
  - la vérification de l'onglet Flux de travaux qui présente l'état de l'instance de processus CA Process Automation et des informations sur la tâche ;
  - la modification de l'état d'une requête, d'une demande de changement ou d'un problème qui entraîne la fin d'un processus CA Process Automation (comme l'annulation d'une demande de changement) ;
  - le choix d'une définition de processus CA Process Automation sur un domaine de demande, une catégorie de changement, une catégorie de problème de CA SDM.

Remarque : Pour plus d'informations sur la configuration de CA EEM, reportez-vous à la documentation de CA Process Automation.

Prise en charge de l'authentification unique de CA SDM vers CA Process Automation en utilisant CA EEM

Quand CA SDM et CA Process Automation sont intégrés, vous pouvez configurer l'authentification unique pour qu'elle fonctionne de CA SDM vers CA Process Automation.

1. Pour cela, vérifiez que les conditions suivantes ont été respectées :
   - LCA SDM et CA Process Automation sont configurés pour utiliser la même installation de CA EEM.
   - L'utilisateur qui se connecte à CA SDM est aussi un utilisateur dans CA Process Automation.
   - Quand CA EEM utilise la base de données interne comme référentiel des utilisateurs, les utilisateurs doivent avoir des autorisations globales ou appartenir au même dossier. Sinon, si CA EEM référence un référentiel externe (comme répertoire externe ou CA SiteMinder), les utilisateurs doivent faire partie du même référentiel pour accéder à l'authentification unique.
2. Installez CA EEM à partir du DVD d'installation de CA SDM ou utilisez toute installation de CA EEM existante (par exemple, CA EEM pour CA Process Automation).

3. Sur l'onglet Administration de CA SDM, installez les options suivantes dans le dossier Sécurité du gestionnaire d'options :
   - eiam_hostname
   - use_eiam_authentication

   Remarque : Il n'est pas nécessaire d'installer l'option caextwf_eem_hostname dans le dossier CA Process Automation du gestionnaire d'options. Mais si vous l'installez, la valeur doit être la même que pour l'option eiam_hostname.
4. Redémarrez CA SDM.
5. Pour créer un utilisateur dans CA Process Automation, procédez comme suit :
   a. Connectez-vous à CA EEM à l'aide du contexte d'application de CA Process Automation en utilisant l'ID d'utilisateur EiamAdmin ou tout autre utilisateur d'administration.
   b. Sélectionnez l'onglet Gérer les identités et cliquez sur l'icône en regard du dossier Utilisateurs.
   c. Le champ Nom situé en haut de la page du nouvel utilisateur est l'ID d'utilisateur qui doit correspondre à l'ID d'utilisateur figurant dans la table des contacts de CA SDM.
   d. Cliquez sur le bouton Ajouter les détails des utilisateurs de l'application et effectuez les opérations suivantes :
      - Ajoutez l'un des groupes, ou les deux groupes, répertoriés. Ajoutez au moins l'un de ces deux groupes afin de pouvoir vous connecter à CA Process Automation.
      - Renseignez les champs du nouvel utilisateur, comme Prénom, Nom, Afficher et Mot de passe.
6. Créez un utilisateur dans la table de contacts de CA SDM avec le même ID d'utilisateur. Assurez-vous que le champ Type de validation de Type d'accès est configuré sur CA EEM pour l'utilisateur.

   Vous pouvez vous connecter à CA EEM et CA SDM avec cet utilisateur et avec le mot de passe spécifié dans CA EEM.

Configuration de la connexion automatique (Authentification de CA MDB)

Pour automatiser le processus de connexion pour les tâches de la liste de travail de CA Workflow lors de l'utilisation des demandes de changement, des demandes, des incidents, des problèmes et des demandes client, vous pouvez configurer la connexion automatique. L'utilisation de la connexion automatique vous évite de devoir entrer un ID utilisateur et un mot de passe lorsque vous cliquez sur le lien d'une liste de travail. La connexion automatique utilise vos informations d'identification de domaine du système d'exploitation Windows pour vous connecter à la liste de travail.

Remarque : Pour que la connexion automatique fonctionne correctement, il n'est *pas* nécessaire d'inclure l'utilisateur dans les groupes Administrateurs de flux de travaux, Initiateurs des processus de flux de travaux ou Superutilisateur Workflow dans CA EEM. Ces groupes fournissent des niveaux d'accès différents aux utilisateurs connectés à CA Workflow Design Environment.

Pour configurer la connexion automatique pour les tâches de la liste de travail (Windows uniquement)

1. Installez et configurez CA Workflow (page 228).
2. Configurez la liste de travail et le gestionnaire de flux de travaux pour la connexion automatique (page 283).
3. Configurez CA EEM pour qu'il utilise la CA MDB pour authentifier les utilisateurs. Lors de l'installation et de la configuration de CA Workflow, votre *nom d'utilisateur de flux de travaux* et votre *mot de passe d'utilisateur de flux de travaux* sont automatiquement ajoutés à CA EEM. Pour obtenir des informations, reportez-vous à la documentation relative à CA EEM.

   Remarque : Un utilisateur doit disposer d'un enregistrement d'utilisateur CA EEM pour accéder à la liste de travail.
4. Connectez-vous à CA SDM et créez une demande de changement, une demande, un incident, un problème ou une demande client avec la catégorie appropriée.

   Remarque : Vérifiez que la catégorie est configurée pour utiliser CA Workflow et comporte une définition CA Workflow liée à l'application avant de créer la demande de changement, la demande, l'incident, le problème ou la demande client.

   Vous pourrez à présent cliquer sur un lien dans la liste de travail et vous connecter sans devoir entrer un ID utilisateur et un mot de passe.

Informations complémentaires :

Configuration de CA Workflow Design Environment pour la connexion automatique (page 284)

Configurer un point d'entrée unique

Quand CA SDM et CA Service Management sont intégrés, un point d'entrée unique permet une authentification unique auprès de CA Service Catalog.

Pour configurer un point d'entrée unique

1. Installez l'option catalog_server General.

   Remarque : Pour plus d'informations, consultez l'Aide en ligne du gestionnaire d'options.

2. Redémarrez CA SDM.
3. Accédez à la page Libre-service employé de CA SDM.
4. Cliquez sur Parcourir les services du catalogue.

   La page de connexion à CA Service Desk Manager s'affiche.

Quand CA EEM est configuré pour CA SDM et pour CA Service Management, un point de contrôle unique peut permettre une authentification unique pour accéder à CA Service Catalog. Quand authentification unique est configurée, la page de connexion à CA Service Management ne s'affiche pas.

Remarque : L'authentification unique n'est pas disponible si vous accédez au libre-service employé de CA SDM en tant qu'invité.

Pour configurer l'authentification unique pour l'accès à CA Service Management

1. Vérifiez que les options de sécurité de CA EEM eiam_hostname et use_eiam_authentication sont installées.
2. Configurez vos utilisateurs dans CA EEM et vérifiez que ces utilisateurs sont aussi des utilisateurs de CA Service Management.
3. Cliquez sur l'onglet Administration.
4. Ouvrez le dossier de gestion des rôles et de la sécurité.
5. Cliquez sur Types d'accès.
6. Sélectionnez le rôle Employé.
7. Vérifiez que, sur l'onglet Authentification Web, le type de validation est défini sur CA EEM-Utiliser CA Embedded Entitlements Manager.
8. Connectez-vous comme l'utilisateur défini de CA EEM et accédez à la page Libre-service employé.
9. Cliquez sur Parcourir les services du catalogue.

   La page principale de CA Service Management s'affiche.

Mise en oeuvre de l'hébergement multiclient

Le *fournisseur de services* est le client hébergé principal d'une installation d'hébergement multiclient CA SDM.

Remarque : Pour de plus amples renseignements sur le fournisseur de services et l'hébergement multiclient, reportez-vous au *Manuel d'administration*.

Vous devez définir les clients hébergés et remplir l'attribut éponyme avec autant d'objets de client hébergé obligatoires et facultatifs que nécessaires avant d'activer l'hébergement multiclient dans un autre mode que le mode de configuration. Pourtant, vous pouvez sélectionner l'application de l'hébergement multiclient avant d'affecter des clients hébergés à tous les objets qui en ont besoin. Les objets avec un client hébergé nul dans une table où les clients hébergés sont obligatoires sont traités comme des objets publics visibles par tous les utilisateurs. L'interface utilisateur détecte et prend en charge toutes les mises à jour réalisées sur ces objets. Selon l'étendue de l'application d'hébergement multiclient, CA SDM peut obliger ou non l'utilisateur à actualiser un objet qui requiert un client hébergé et à fournir un client hébergé.

Remarque : Vous devez créer un client hébergé avant qu'une instance d'objet avec client hébergé obligatoire puisse être mise à jour. Par ailleurs, les utilitaires pdm_settenant et pdm_buildtenant peuvent être utilisés après l'activation de l'hébergement multiclient pour remplir le paramètre de l'attribut. Si, par erreur, les tables avec client hébergé obligatoire contiennent des données non hébergées dans un système d'hébergement multiclient, une liste déroulante de données publiques s'affiche dans les tables avec client hébergé obligatoire.

Important : Avant d'exécuter pdm_buildtenant, vous *devez* configurer le fournisseur de services.

Pour mettre en oeuvre l'hébergement multiclient, effectuez les opérations suivantes :

1. Définissez l'option Hébergement multiclient sur "setup." (page 323) et redémarrez CA SDM. Vous devez lancer le cycle des services à chaque fois que vous modifiez l'état du client hébergé (configuration, activé, activé(autoriser)).

   Important : Lorsque l'hébergement multiclient est en mode de configuration, les modifications d'interface Web sont actives pour les administrateurs des fournisseurs de services, permettant l'affichage et la modification des objets et données liés au client hébergé sur l'interface Web. Cependant, les restrictions d'hébergement ne sont pas appliquées et les utilisateurs (autres que les administrateurs des fournisseurs de services) ne voient pas les modifications d'interface du produit. Vous pouvez donc continuer à utiliser le produit en mode non hébergé pendant sa préparation pour l'hébergement multiclient.

2. Mappez toute mise en oeuvre de client hébergé existante à l'objet de client hébergé. (page 325)

3. Remplissez les colonnes Client hébergé (page 326).

   Remarque : Il est recommandé de commencer par remplir la colonne Client hébergé dans les contacts, puis d'utiliser les contacts avec client hébergé pour remplir la colonne Client hébergé dans les autres objets.

4. Vérifiez que le client hébergé est défini dans toutes les tables avec client hébergé obligatoire.

5. Créez des clients hébergés. (page 327)

   Important : Le premier client hébergé que vous créez doit être le client hébergé par le fournisseur de services. Après avoir créé le client hébergé par le fournisseur de services, déconnectez-vous de CA Service Desk et connectez-vous à nouveau en tant que membre du fournisseur de services. Connectez-vous en tant qu'utilisateur à forts privilèges (par exemple, ServiceDesk), car cet utilisateur appartient automatiquement au client hébergé par le fournisseur de services. Si vous souhaitez vous connecter en tant que contact différent, utilisez d'abord pdm_settenant pour affecter le contact au fournisseur de services.

6. Créer des groupes de clients hébergés (page 329)

7. Définissez l'option Hébergement multiclient sur "on". (page 323)

   Après la sélection de cette option, redémarrez les services et exécutez les étapes suivantes.

   a. Connectez-vous en utilisant le nom d'utilisateur à forts privilèges (généralement *ServiceDesk*).

   b. Vérifiez que l'utilisateur à forts privilèges est affecté au client hébergé du fournisseur de services.

   c. Vérifiez que vos restrictions d'hébergement multiclient sont appliquées.

   Important : Si des données sans client hébergé restent dans la base de données, vous pouvez définir l'application d'hébergement multiclient sur *avertir* ou *autoriser*. Ceci permet des mises à jour des tables avec client hébergé obligatoire avec un client hébergé nul. La perte de données est ainsi évitée lorsqu'un accord sur les niveaux de service (SLA) ou un événement joint s'exécute sur un billet qui n'a pas encore été mis à jour pour contenir un client hébergé.

   Remarque : Vous pouvez exécuter pdm_settenant même après l'activation de l'hébergement multiclient pour contrôler que la mise en oeuvre est bien terminée (avec l'option -r) et pour mettre à jour en masse le client hébergé selon les besoins.

8. Sauvegardez les contraintes et les rôles de partition de données.

   L'hébergement multiclient réduit le nombre et la complexité des contraintes de partition de données obligatoires, leur permettant ainsi d'être simplifiées. Avant de réaliser des modifications, faites une sauvegarde des tables Domain_Constraint et usp_role.

9. Supprimez les contraintes de partition de données inutiles.

   De nombreuses contraintes de domaine définies pour l'hébergement unique ne sont plus nécessaires après l'activation de l'hébergement multiclient et peuvent donc être supprimées. La suppression de ces contraintes améliore les performances des requêtes.

10. Passez en revue vos modifications et exécutez une vérification.

    Exécutez *pdm_settenant -r* pour vérifier si des clients hébergés supplémentaires sont nécessaires dans les tables avec client hébergé obligatoire. Vérifiez s'il est nécessaire d'ajouter des hébergements aux tables avec client hébergé facultatif, par exemple Catégorie et Notification d'activité.

11. (Facultatif) Désactivez l'hébergement multiclient si des problèmes surviennent. Si vous rencontrez des problèmes après la mise en oeuvre, vous pouvez exécuter les étapes suivantes manuellement :

    a. Restaurez les tables Domain_Constraint et usp_role.

    b. Définissez de nouveau l'option Hébergement multiclient sur "configuration".

    c. Redémarrez le système.

    Le site peut reprendre des opérations précédentes pendant que vous continuez à remplir les colonnes Client hébergé et corrigez les problèmes qui nécessitaient la restauration.

Remarque : Si les tables qui requièrent un client hébergé contiennent à tort des données sans client hébergé dans un système d'hébergement multiclient, une liste déroulante des données publiques apparaît dans les tables qui requièrent un client hébergé et un message AHD05358 indiquant que *nn* objets *xxx* actifs sans client hébergé ont été détectés au démarrage du Centre de services s'affiche.

Hébergement multiclient

L'hébergement multiclient permet à plusieurs clients indépendants (*clients hébergés*) et à leurs utilisateurs de partager une mise en oeuvre unique du produit. Les clients hébergés partagent des ressources matérielles et d'application, réduisant ainsi le coût des deux types de ressources.

Les utilisateurs de client hébergé ne communiquent entre eux que de manière définie, comme spécifié par leurs *rôles* et les *hiérarchies de clients hébergés.*

- **Rôle** : Le rôle d'un utilisateur CA SDM contrôle l'autorisation d'accès. L'ensemble de rôles auxquels les utilisateurs ont accès dépendent de leur type d'accès. L'hébergement multiclient vous permet de contrôler le client hébergé ou le groupe de clients hébergés auquel un utilisateur peut accéder dans le rôle.

- **Hiérarchie de clients hébergés** : il s'agit d'un groupe structuré de clients hébergés, créé par le système ou modifié lorsque vous affectez un client hébergé parent à un client hébergé. Le client hébergé devient un client hébergé fils des clients hébergés parents et supérieurs (le cas échéant) dans cette hiérarchie.

En règle générale, chaque client hébergé affiche la mise en oeuvre pour un usage exclusif. Un client hébergé ne peut pas mettre à jour ou afficher les données d'un autre client hébergé.

Client hébergé de fournisseur de services

Un *fournisseur de services* fournit des services à d'autres entités. Dans une mise en oeuvre d'hébergement multiclient, le fournisseur de services est le client hébergé principal (propriétaire) et gère d'autres clients hébergés.

Seul le client hébergé de fournisseur de services peut effectuer les tâches suivantes :

- Définir les options CA SDM
- Définir les options Gestion des connaissances
- Définir les options de l'Automatisation du soutien
- Créer des tables ou des colonnes
- Créer, modifier ou supprimer des clients hébergés
- Permettre aux clients hébergés d'avoir des clients hébergés secondaires
- Mettre à jour des données publiques

Hiérarchies des clients hébergés

Une *hiérarchie des clients hébergés* est un groupe de clients hébergés structuré qui est créé par le système ou modifié lorsque vous affectez un *client hébergé parent* à un client hébergé. Le client hébergé devient un *client hébergé fils* des clients hébergés parents et supérieurs (le cas échéant) dans cette hiérarchie. Un *client hébergé père* est un client hébergé supérieur à un autre client hébergé (son *client hébergé fils relatif*) dans la même hiérarchie de clients hébergés. Un client hébergé fils représente généralement une subdivision à l'intérieur de ses clients hébergés pères. Un client hébergé fils peut avoir ses propres règles et données commerciales, et les données du client hébergé père sont "transférées" automatiquement vers le client hébergé fils en lecture seule.

Le produit prend en charge une hiérarchie de clients hébergés de profondeur illimitée. Toutefois, le fournisseur de services peut spécifier une limite pour le nombre total de clients hébergés et la profondeur des hiérarchies de clients hébergés. Par défaut, la limite est de quatre niveaux. Le fournisseur de services détermine aussi si des clients hébergés spécifiques peuvent avoir des clients hébergés fils. Le fournisseur de services peut également appartenir à des hiérarchies de clients hébergés. Le fournisseur de services ne peut pas avoir de client hébergé parent.

Remarque : Le fournisseur de services peut créer de multiples hiérarchies non associées ou n'en créer aucune. Même dans un système avec des hiérarchies de clients hébergés, vous pouvez définir des clients hébergés autonomes.

Attributs et objets de client hébergé

Lors de l'activation de l'hébergement multiclient, vous pouvez octroyer à chaque contact (utilisateur) l'accès à : tous les clients hébergés (public), un seul client hébergé, ou un groupe de clients hébergés (défini par l'utilisateur ou géré par le système). Le rôle d'un contact contrôle l'accès, qui spécifie l'accès en lecture et en écriture indépendamment. L'accès au client hébergé étant tributaire du rôle et un contact pouvant changer de rôles pendant une session, l'accès au client hébergé de contact peut également être modifié.

Dans une mise en oeuvre d'hébergement multiclient, la plupart des objets incluent un attribut de client hébergé qui spécifie le client hébergé propriétaire de l'objet. Les objets sont répartis entre les groupes suivants, en fonction de leur attribut de client hébergé et de leur utilisation :

Sans client hébergé

Définit les objets sans attribut de client hébergé. Toutes les données de ces objets sont publiques.

Exemples : Priorité et urgence

Client hébergé obligatoire

Définit les objets avec un attribut de client hébergé ne pouvant pas être nul. C'est le produit et non le système de gestion de bases de données qui applique cette restriction. Toutes les données dans ces objets sont associées à des clients hébergés spécifiques ; il n'existe aucune donnée publique.

Exemples : Tables de billet (Demande, Demande client et Demande de changement).

Client hébergé facultatif

Définit les objets avec un attribut de client hébergé pouvant être nul. Certaines des données de ces objets sont publiques et d'autres sont associées à des clients hébergés spécifiques. Chaque client hébergé affiche l'objet dans une vue fusionnée reprenant des données publiques et ses données spécifiques.

Exemples : Catégorie et emplacement

Accès Hébergement multiclient

Lorsqu'un utilisateur interroge la base de données, le produit limite les résultats aux objets appartenant aux clients hébergés auxquels l'utilisateur peut accéder. Cette restriction s'applique par ailleurs à toute restriction de partition de données en vigueur. Les utilisateurs voient uniquement les données des tables avec client hébergé obligatoire et client hébergé facultatif ainsi que les données appartenant aux clients hébergés auxquels ils peuvent accéder.

Lorsqu'un utilisateur de client hébergé demande de créer ou de mettre à jour un objet de base de données, le produit vérifie les éléments suivants :

- L'objet appartient à un client hébergé dont la mise à jour est autorisée par le rôle actuel de l'utilisateur.
- Toutes les références de clé étrangère (SREL) de l'objet vers d'autres objets sont de l'un des types suivants :
  - Objets publics (sans client hébergé)
  - Objets du même client hébergé
  - Objets de clients hébergés dans la hiérarchie de clients hébergés situés au-dessus de l'objet du client hébergé. En d'autres termes, un objet de client hébergé peut référencer des objets appartenant à son client hébergé parent, au parent de son parent, et ainsi de suite.

  Remarque : Il existe une exception à la restriction de référence SREL. Certaines références SREL (telles que le destinataire d'un incident) peuvent référencer des objets qui appartiennent à des clients hébergés dans la hiérarchie de clients hébergés de l'objet conteneur. Ces références sont désignées comme SERVICE_PROVIDER_ELIGIBLE dans le schéma d'objet du produit. L'indicateur SERVICE_PROVIDER_ELIGIBLE marque une différence uniquement si le client hébergé du fournisseur de services ne se trouve pas au-dessus de l'objet du client hébergé dans la hiérarchie de clients hébergés. Lorsque le client hébergé du fournisseur de services se trouve dans la hiérarchie, les règles de validation de client hébergé autorisent les références de fournisseur de services.

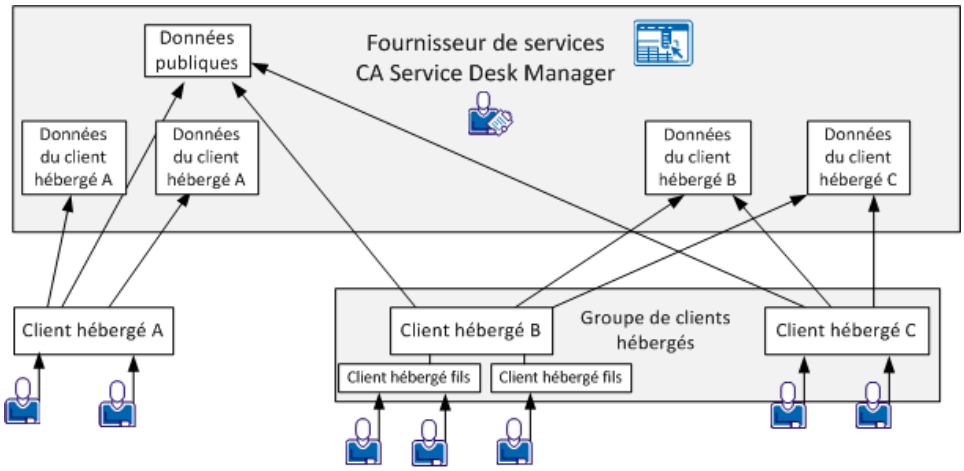
Si un utilisateur qui crée un objet a un accès de mise à jour aux clients hébergés multiples, il doit spécifier le client hébergé explicitement, directement ou indirectement.

Un utilisateur de fournisseur de services demandant la création ou la mise à jour d'un objet est soumis aux mêmes restrictions que les utilisateurs de client hébergé. L'exception est que vous pouvez autoriser les utilisateurs de fournisseur de services à créer ou à mettre à jour des objets publics. Le rôle activé de l'utilisateur de fournisseur de services contrôle cette autorisation.

Remarque : Si le produit ne permet pas à un utilisateur de mettre à jour les données d'un client hébergé, un message d'erreur peut annoncer une restriction de la partition de données. Si vous recevez ce message d'erreur, les restrictions relatives à la partition de données ou à l'hébergement multiclient sont en vigueur.

Exemple : Accès de client hébergé aux données CA SDM

Cet exemple illustre l'accès des clients hébergés A, B et C aux données leur appartenant et aux données publiques dans CA SDM.



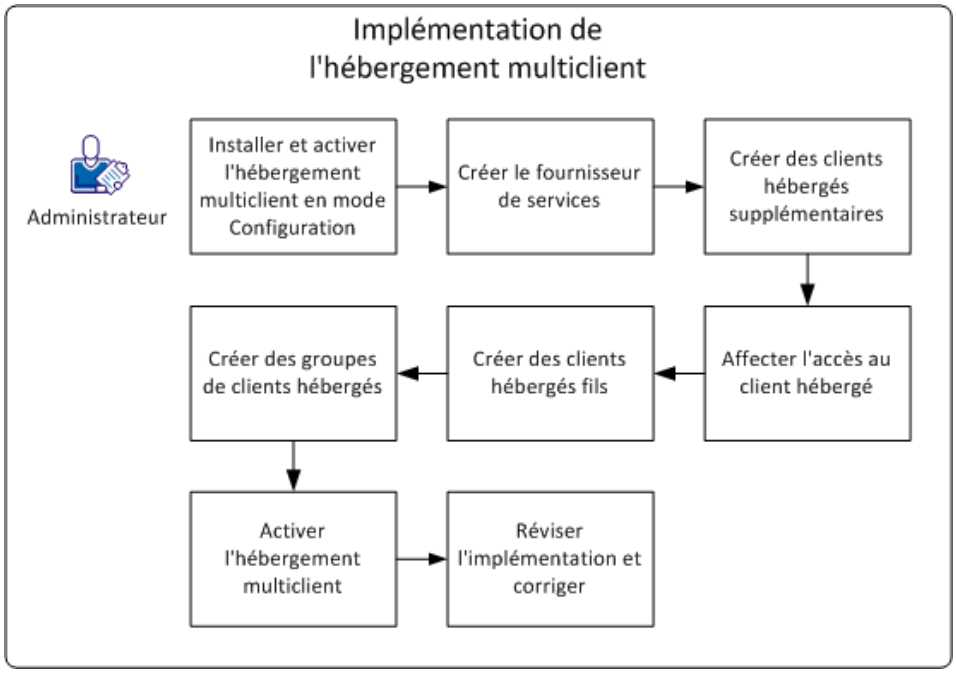
Dans cet exemple, les flèches pointent vers des données auxquelles chaque client hébergé peut accéder comme suit :

- Les utilisateurs du client hébergé A peuvent accéder aux données du client hébergé A et aux données publiques.
- Le client hébergé B et ses utilisateurs de client hébergé fils peuvent accéder aux données du client hébergé B et aux données publiques.
- Les utilisateurs du client hébergé C peuvent accéder aux données du client hébergé C et aux données publiques.
- Les utilisateurs peuvent afficher les données publiques et les données des clients hébergés B et C, car le client hébergé B, ses clients hébergés fils et le client hébergé C appartiennent à un groupe de clients hébergés.

Mise en oeuvre de l'hébergement multiclient

Le diagramme suivant décrit la première mise en oeuvre par un administrateur, en tant qu'utilisateur à forts privilèges CA SDM, de l'hébergement multiclient. Du début à la fin, la mise en oeuvre de CA SDM est modifiée comme suit :

1. Un client unique utilise une mise en oeuvre unique.
2. Plusieurs clients indépendants (clients hébergés) et leurs utilisateurs *partagent* une mise en oeuvre unique. Chaque client hébergé affiche la mise en oeuvre pour un usage exclusif.


Implémentation de l'hébergement multiclient
Administrateur
Installer et activer l'hébergement multiclient en mode Configuration
Créer le fournisseur de services
Créer des clients hébergés supplémentaires
Affecter l'accès au client hébergé
Créer des clients hébergés fils
Créer des groupes de clients hébergés
Activer l'hébergement multiclient
Réviser l'implémentation et corriger

En tant qu'administrateur, utilisez l'interface d'administration CA SDM pour effectuer les étapes suivantes :

1. Installer et activer l'hébergement multiclient en mode Configuration (page 311)
2. Créer le client hébergé fournisseur de services (page 312)
3. Créer des clients hébergés supplémentaires (page 314)
4. Affecter un accès de client hébergé pour un rôle (page 316)
5. Créer des clients hébergés fils (page 319)
6. Créer des groupes de clients hébergés (page 319)
7. Activer l'hébergement multiclient (page 321)et redémarrer les services
8. Vérifier la mise en oeuvre et résoudre (page 322)les éventuels problèmes

Installation et activation de l'hébergement multiclient

Pour activer l'hébergement multiclient, installez une option d'hébergement multiclient dans le produit, puis activez le mode de configuration. Le mode de configuration spécifie que les fonctionnalités d'hébergement multiclient sont actives pour les administrateurs. Ce mode permet d'afficher et de modifier des objets et des attributs liés aux clients hébergés. Cependant, le produit n'applique pas les restrictions de client hébergé et les utilisateurs non-administrateurs ne voient aucune modification. Ce mode permet de préparer l'hébergement multiclient en effectuant des tâches telles que la définition de clients hébergés ou l'affectation des clients hébergés à des rôles sans altérer l'utilisation normale du produit.

Important : Lorsque l'hébergement multiclient est en mode de configuration, les modifications d'interface Web sont activées pour les administrateurs de fournisseurs de services. Ce comportement permet d'afficher et de modifier des données et objets liés aux clients hébergés dans l'interface Web. Cependant, les restrictions d'hébergement ne sont pas appliquées et les utilisateurs (autres que les administrateurs des fournisseurs de services) ne voient pas les modifications d'interface du produit. Par conséquent, vous pouvez continuer d'utiliser le produit lors de la mise en oeuvre de l'hébergement multiclient.

1. Connectez-vous à CA SDM en tant qu'administrateur et cliquez sur l'onglet Administration.
2. Dans l'arborescence à gauche, cliquez sur Gestionnaire d'options, Hébergement multiclient.

   La page Liste des options s'affiche.
3. Cliquez sur Hébergement multiclient.

   La page Détail des options de l'hébergement multiclient apparaît.
4. Cliquez sur Modifier.

   La page Mettre à jour les options s'affiche.
5. Dans la liste déroulante Valeur de l'option, Sélectionnez Configuration.
6. Cliquez sur Installer.

   L'option Hébergement multiclient est maintenant installée.

7. Cliquez sur Actualiser.

   La page affiche vos modifications.

8. Fermez la fenêtre.

   La page Liste des options s'affiche à nouveau.

9. Redémarrez les services.

   L'hébergement multiclient est prêt pour la mise en oeuvre en mode de configuration.

Création du client hébergé de fournisseur de services

Utilisez le produit pour créer le client hébergé de fournisseur de services. Lors de la création du premier client hébergé, les événements suivants se produisent :

1. Le premier client hébergé devient toujours le fournisseur de services.

   Important : Vous ne pouvez pas modifier cette identification : dans la page Créer un client hébergé, la case à cocher Fournisseur de services et le champ État de l'enregistrement sont en lecture seule.

2. Le produit associe l'utilisateur à forts privilèges (en règle générale ServiceDesk sous Windows ou srvcdesk sous Linux/UNIX) au client hébergé du fournisseur de services. Le produit définit tous les contacts système (tels que System_AHD_Generated) de sorte qu'ils appartiennent au nouveau client hébergé de fournisseur de services.

   Remarque : Windows fournit un utilisateur système Administrateur. L'utilisateur à forts privilèges doit affecter manuellement un client hébergé à l'administrateur.

1. Sélectionnez Gestion des rôles et de la sécurité, Clients hébergés sous l'onglet Administration.

   La page Liste de clients hébergés s'affiche.

   Remarque : L'option Gestion des rôles et de la sécurité, Clients hébergés est disponible uniquement si l'hébergement multiclient est installé et en mode de configuration ou d'activation.

2. Cliquez sur Créer.

   La page Créer un client hébergé s'affiche.

3. Remplissez les champs suivants :

   Nom

   Affiche le nom du client hébergé.

   Fournisseur de services

   Identifie si ce client hébergé est le fournisseur de services.

Numéro du client hébergé

(À titre d'information uniquement) Affiche le numéro du client hébergé. CA SDM n'utilise pas cette option.

État de l'enregistrement

Configure le client hébergé sur Activé ou Désactivé.

Client hébergé parent

Spécifie un autre client hébergé au-dessus de ce client hébergé, en faisant de ce dernier un client hébergé fils dans une hiérarchie de clients hébergés.

Clients hébergés fils autorisés

Permet à ce client hébergé d'avoir des clients hébergés fils. Le client hébergé ne peut pas modifier le paramètre.

Profondeur du client hébergé

(À titre d'information uniquement) Indique la profondeur de ce client hébergé.

Groupe de clients hébergés pères

(À titre d'information uniquement) Identifie le groupe de clients hébergés géré par le système et qui contient ce client hébergé et tous les clients hébergés qui lui sont supérieurs dans la hiérarchie.

Groupe de clients hébergés fils

(À titre d'information uniquement) Identifie le groupe de clients hébergés géré par le système et qui contient ce client hébergé et tous les clients hébergés qui lui sont inférieurs dans la hiérarchie.

Groupe de clés étrangères

(À titre d'information uniquement) Identifie le groupe de clients hébergés géré par le système et qui contient des clients hébergés pouvant être référencés à partir d'une SREL dans des données qui appartiennent à ce client hébergé. Le groupe de clés étrangères est identique au groupe de clients hébergés pères.

Groupe de clients hébergés associés

(À titre d'information uniquement) Identifie le groupe de clients hébergés géré par le système et qui comprend aussi bien des groupes de clients hébergés pères que des groupes de clients hébergés fils pour ce client hébergé.

Conditions d'utilisation

Spécifie les conditions d'utilisation pour le client hébergé.

Logo

Spécifie l'adresse URL du fichier de logo du client hébergé, qui peut être un type quelconque d'image Web.

Emplacement

Affiche la page de recherche d'emplacement, qui permet de spécifier un emplacement.

Contact

Affiche la page de recherche de contact, qui permet de spécifier un contact.

Remarque : Si aucun contact n'est associé au client hébergé respectif, les champs Adresse de courriel et Adresse de courriel du téléavertisseur sont désactivés.

4. Cliquez sur Enregistrer.

   Le produit crée le client hébergé de fournisseur de services.

5. Fermez la fenêtre.
6. Cliquez avec le bouton droit de la souris sur Liste de clients hébergés et sélectionnez Actualiser.

   La Liste de clients hébergés est actualisée et contient le client hébergé de fournisseur de services créé.

7. Déconnectez-vous de CA SDM.

Création de clients hébergés

Utilisez le produit pour créer d'autres clients hébergés. Vous pouvez créer autant de clients hébergés que nécessaire pour gérer plusieurs entreprises distinctes qui fournissent un soutien à des clients.

1. Connectez-vous à l'interface d'administration en tant que membre du fournisseur de services. Une manière simple d'établir cette connexion consiste à se connecter en tant qu'utilisateur à forts privilèges (par exemple : ServiceDesk). Cet utilisateur appartient automatiquement au client hébergé du fournisseur de services.
2. Sélectionnez Gestion des rôles et de la sécurité, Clients hébergés sous l'onglet Administration.

   La page Liste de clients hébergés s'affiche.

   Remarque : L'option Gestion des rôles et de la sécurité, Clients hébergés est disponible uniquement si l'hébergement multiclient est installé et en mode de configuration ou d'activation.

3. Cliquez sur Créer.

   La page Créer un client hébergé s'affiche.

4. Remplissez les champs comme suit :

   Nom

   Affiche le nom du client hébergé.

Fournisseur de services

Identifie si un client hébergé est le fournisseur de services. Le premier client hébergé créé est toujours le fournisseur de services ; par conséquent cette case à cocher est en lecture seule.

Numéro du client hébergé

(À titre d'information uniquement) Affiche le numéro du client hébergé. CA SDM n'utilise pas cette option.

État de l'enregistrement

Configure le client hébergé sur Activé ou Désactivé.

Client hébergé parent

Spécifie un autre client hébergé au-dessus de ce client hébergé, en faisant de ce dernier un *client hébergé fils* dans une hiérarchie de clients hébergés.

Clients hébergés fils autorisés

Permet à ce client hébergé d'avoir des clients hébergés fils. Le client hébergé ne peut pas modifier le paramètre.

Profondeur du client hébergé

(À titre d'information uniquement) Indique la profondeur de ce client hébergé.

Groupe de clients hébergés pères

(À titre d'information uniquement) Identifie le groupe de clients hébergés géré par le système et qui contient ce client hébergé et tous les clients hébergés qui lui sont supérieurs dans la hiérarchie.

Groupe de clients hébergés fils

(À titre d'information uniquement) Identifie le groupe de clients hébergés géré par le système et qui contient ce client hébergé et tous les clients hébergés qui lui sont inférieurs dans la hiérarchie.

Groupe de clés étrangères

(À titre d'information uniquement) Identifie le groupe de clients hébergés géré par le système et qui contient des clients hébergés pouvant être référencés à partir d'une SREL dans des données qui appartiennent à ce client hébergé. Le groupe de clés étrangères est identique au groupe de clients hébergés pères.

Groupe de clients hébergés associés

(À titre d'information uniquement) Identifie le groupe de clients hébergés géré par le système et qui comprend aussi bien des groupes de clients hébergés pères que des groupes de clients hébergés fils pour ce client hébergé.

Conditions d'utilisation

Spécifie les conditions d'utilisation pour le client hébergé.

Logo

Spécifie l'adresse URL du fichier de logo du client hébergé, qui peut être un type quelconque d'image Web.

Emplacement

Affiche la page de recherche d'emplacement, qui permet de spécifier un emplacement.

Contact

Affiche la page de recherche de contact, qui permet de spécifier un contact.

Remarque : Si aucun contact n'est associé au client hébergé respectif, les champs Adresse de courriel et Adresse de courriel du téléavertisseur sont désactivés.

5. Cliquez sur Enregistrer.

   Le produit crée le client hébergé.

6. Fermez la fenêtre.

7. Cliquez avec le bouton droit de la souris sur Liste de clients hébergés et sélectionnez Actualiser.

   La Liste des clients hébergés est actualisée et affiche le client hébergé créé.

8. (Facultatif) Pour chaque client hébergé que vous voulez créer, répétez les étapes 3 à 6.

Affectation de l'accès de client hébergé pour un rôle

Le rôle d'un utilisateur de CA SDMcontrôle l'autorisation d'accès et l'interface utilisateur. Les rôles disponibles pour les utilisateurs dépendent de leur type d'accès. L'hébergement multiclient vous permet de contrôler le client hébergé ou le groupe de clients hébergés auquel un utilisateur peut accéder dans le rôle. Lorsque l'hébergement multiclient est installé, la page de détail du rôle inclut des options supplémentaires qui permettent d'affecter ou de modifier l'accès de client hébergé.

Remarque : Vous pouvez permettre aux d'utilisateurs de client hébergé d'accéder à d'autres données que les leurs. Les analystes de client hébergé autre que le fournisseur de services disposent uniquement d'un accès à leurs propres client hébergé et clients hébergés fils. Toutefois, vous pouvez mettre à jour leur accès aux fonctions pour inclure le client hébergé de l'analyste. Par exemple, vous pouvez définir un rôle pour configurer un accès en lecture et en écriture séparé à certains groupes de clients pour des utilisateurs de ce rôle.

1. Accédez à Gestion des rôles et de la sécurité, Gestion des rôles, Liste des rôles.

   La liste des rôles s'affiche.

2. Cliquez sur le rôle auquel vous voulez affecter l'accès de client hébergé.

   La page de détail du rôle s'affiche et contient les listes déroulantes Accès au client hébergé et Droits d'accès en écriture du client hébergé sous l'onglet Autorisation. L'accès au client hébergé est en lecture seule et les droits d'accès en écriture du client hébergé autorisent également la création et la mise à jour.

3. Cliquez sur Modifier.

   La page Mettre à jour le rôle s'affiche.

4. Sélectionnez des options pour l'accès du client hébergé et les droits d'accès en écriture du client hébergé :

   Identique à l'accès au client hébergé

   Définit l'accès pour qu'il soit identique à l'accès au client hébergé. Il s'agit de la valeur par défaut de la liste déroulante Droits d'accès en écriture du client hébergé. Elle est uniquement disponible pour l'option Droits d'accès en écriture du client hébergé.

   Tous les clients hébergés

   Supprime les restrictions de client hébergé. Dans un rôle, l'utilisateur disposant de cet accès peut effectuer les actions suivantes :

   - Affichage d'un objet dans la base de données (droits d'accès en lecture).
   - Création et mise à jour (droits d'accès en écriture) d'un objet avec client hébergé dans la base de données

   Lorsqu'un utilisateur disposant d'un accès à tous les clients hébergés crée un objet, il doit sélectionner le client hébergé du nouvel objet.

   Client hébergé unique

   Définit l'accès de client hébergé d'un rôle sur un client hébergé nommé. Lorsque vous sélectionnez cette option, un autre champ s'affiche et permet de sélectionner un client hébergé spécifique. Un utilisateur de ce rôle ne peut accéder qu'aux objets associés au client hébergé nommé.

   Groupe de clients hébergés

   Définit l'accès au client hébergé d'un rôle à un groupe de clients hébergés défini par l'utilisateur ou géré par le système. Après la sélection de cette option, un autre champ permet de sélectionner un client hébergé spécifique. Un utilisateur de ce rôle peut accéder uniquement aux objets associés à l'un des clients hébergés de ce groupe. Lorsqu'un utilisateur disposant d'un accès au groupe de clients hébergés crée un objet, il doit sélectionner le client hébergé du nouvel objet.

   Client hébergé du contact

   Définit l'accès d'un rôle au client hébergé du contact l'utilisant. Un utilisateur de ce rôle peut accéder uniquement aux objets associés à son propre client hébergé.

Groupe de clients hébergés du contact

Définit l'accès d'un rôle d'analyste au groupe de clients hébergés que l'analyste utilise, comme spécifié dans l'enregistrement de contact de l'analyste. Si l'utilisateur avec le rôle n'est pas un analyste, cette sélection a le même effet que le client hébergé du contact. Cette option est disponible uniquement pour les analystes.

Groupe de clients hébergés fils du contact

Définit l'accès d'un rôle au groupe de clients hébergés fils du contact l'utilisant. Un utilisateur de ce rôle peut accéder uniquement aux objets associés à son propre groupe de clients hébergés fils.

Groupe de clients hébergés pères du contact

Définit l'accès d'un rôle au groupe de clients hébergés pères du contact l'utilisant. Un utilisateur de ce rôle peut accéder uniquement aux objets associés à son propre groupe de clients hébergés pères.

Groupe de clients hébergés associés du contact

Définit l'accès d'un rôle au groupe de clients hébergés associés du contact l'utilisant. Un utilisateur de ce rôle peut accéder uniquement aux objets associés à son propre groupe de clients hébergés associés.

Mettre à jour les données publiques

Détermine si un utilisateur du fournisseur de services dans le rôle est autorisé à créer ou à mettre à jour des données publiques. Tous les utilisateurs peuvent afficher des données publiques, indépendamment des droits d'accès pour le rôle actuel. Les utilisateurs de client hébergé (utilisateurs appartenant à un client hébergé autre que le fournisseur de services) ne peuvent pas mettre à jour des données publiques, quel que soit leur rôle.

Cliquez sur Enregistrer.

L'accès au client hébergé est affecté au rôle. Lorsqu'un utilisateur interroge la base de données, le produit limite les résultats aux objets appartenant aux clients hébergés associés au rôle de l'utilisateur.

Création de clients hébergés fils

L'hébergement de clients fils permet de définir et de modifier des hiérarchies de clients hébergés à des fins organisationnelles et de partage de données. Pour placer un client hébergé dans une hiérarchie de clients hébergés, affectez-lui un client hébergé parent.

1. Sous l'onglet Administration, sélectionnez Gestion des rôles et de la sécurité, Clients hébergés.

   La liste des clients hébergés s'affiche.

   Remarque : L'option Clients Hébergés dans Gestion des rôles et de la sécurité est disponible uniquement lorsque l'hébergement multiclient est activé.

2. Cliquez sur un client hébergé existant à modifier, ou cliquez sur Créer.

   La page Détail du client hébergé s'affiche et permet d'entrer les données ou modifications requises.

3. Sélectionnez un client hébergé parent.

   Remarque : La liste déroulante Client hébergé parent affiche uniquement les clients hébergés autorisés à disposer de clients hébergés fils.

4. Cliquez sur Enregistrer.

   Le client hébergé est un client hébergé fils du client hébergé parent.

   Remarque : Lorsqu'un client hébergé est un client hébergé fils, il appartient au groupe de clients hébergés fils du client hébergé parent. Le client hébergé parent rejoint le groupe de clients hébergés pères du client hébergé fils. Chaque client hébergé rejoint le groupe des clients hébergés associés de l'autre.

Création de groupes de clients hébergés

Un groupe de clients hébergés consiste en un ensemble de clients hébergés qui partagent l'accès aux objets CA SDM. Les groupes de clients hébergés permettent de classer, de gérer et de contrôler l'accès aux clients hébergés. Vous pouvez affecter un rôle à un client hébergé ou à un groupe de clients hébergés. Lorsque l'hébergement multiclient est activé, le produit associe chaque rôle avec tous les clients hébergés (publics), un client hébergé unique, ou un groupe de clients hébergés unique. Utilisez des groupes de clients hébergés lorsqu'un rôle requiert l'accès à plusieurs clients hébergés. Par exemple, vous pouvez affecter des analystes à un groupe contenant des clients hébergés appartenant à une zone géographique spécifique.

Le produit génère et gère automatiquement trois groupes de clients hébergés pour chaque client hébergé dans une hiérarchie de clients hébergés (*client-hébergé* est le nom du client hébergé) :

- *client-hébergé*_clients-hébergés-fils (client hébergé, ses clients hébergés enfants et leurs clients hébergés fils inférieurs)
- *client-hébergé*_clients-hébergés-pères (client hébergé, son client hébergé parent et ses clients hébergés pères supérieurs)
- *client-hébergé*_clients-hébergés-associés (hiérarchie complète unique)

Utilisez les groupes de clients hébergés gérés par le système comme groupes de clients hébergés définis par l'utilisateur. Toutefois, vous pouvez uniquement modifier les noms des groupes de clients hébergés gérés par le système et les descriptions.

Exemple : Le rôle A requiert l'accès au client hébergé A, au client hébergé B et au client hébergé J.

Au lieu d'affecter le rôle à chaque client hébergé séparément, vous pouvez procéder comme suit :

1. Créez un groupe de clients hébergés et ajoutez le client hébergé A, le client hébergé B et le client hébergé J au groupe.
2. Affectez le rôle A à ce groupe de clients hébergés.

   Les utilisateurs (contacts) affectés au rôle A peuvent accéder au groupe de clients hébergés, qui comprend les clients hébergés A, B et J.

1. Connectez-vous en tant que fournisseur de services, cliquez sur l'onglet Administration et sélectionnez Gestion des rôles et de la sécurité.
2. Cliquez sur Groupes de clients hébergés.

   La liste des groupes de clients hébergés s'affiche.

   Remarque : L'option Groupes de clients hébergés dans Gestion des rôles et de la sécurité est disponible uniquement lorsque l'hébergement multiclient est installé (activé ou configuré).
3. Cliquez sur Créer.

   La page Créer un groupe de clients hébergés s'affiche.
4. Remplissez les champs suivants :

   Nom du groupe de clients hébergés

   Affiche le nom du groupe de clients hébergés sélectionné.

   État de l'enregistrement

   Définit le groupe de clients hébergés comme activé ou désactivé

Description

Affiche une description du groupe de clients hébergés.

5. Cliquez sur Enregistrer.

   Le groupe de clients hébergés est créé.

6. Fermez la fenêtre.

   La liste des groupes de clients hébergés s'affiche.

7. Cliquez avec le bouton droit de la souris sur Liste de clients hébergés et sélectionnez Actualiser.

   La liste des groupes de clients hébergés est mise à jour.

8. Sur la page Détails du groupe de clients hébergés, cliquez sur Mettre à jour les clients hébergés et ajoutez des membres de client hébergé au groupe.

9. (Facultatif) Pour chaque groupe de clients hébergés que vous voulez créer, répétez les étapes 3 à 6.

Modification de l'hébergement multiclient en mode d'activation

Vous pouvez modifier l'option Hébergement multiclient en mode d'activation pour rendre complète la fonction de mise en oeuvre d'hébergement multiclient. Ainsi, chaque client hébergé affiche la mise en oeuvre pour un usage exclusif. Un client hébergé ne peut pas mettre à jour ou afficher les données d'un autre client hébergé.

1. Connectez-vous à CA SDM en tant qu'administrateur et cliquez sur l'onglet Administration.

2. Dans l'arborescence à gauche, cliquez sur Gestionnaire d'options, Hébergement multiclient.

   La page Liste des options s'affiche.

3. Cliquez sur Hébergement multiclient.

   La page Détail des options de l'hébergement multiclient apparaît.

4. Cliquez sur Modifier.

   La page Mettre à jour les options s'affiche.

5. Dans la liste déroulante Valeur de l'option, Sélectionnez Configuration.

6. Cliquez sur Modifier.

   La page Mettre à jour les options s'affiche.

7. Parmi les valeurs suivantes de la liste déroulante Valeur de l'option, sélectionnez Activé (valeur par défaut) :

   Activé

   (Valeur par défaut) Empêche l'archivage d'une table avec client hébergé obligatoire lorsque le client hébergé a une valeur nulle et qu'un attribut SREL d'une table avec un client hébergé n'est pas disponible.

   Activé (avertissement)

   Écrit une erreur dans le journal mais autorise l'archivage, lorsqu'un objet avec client hébergé obligatoire est créé ou mis à jour avec une valeur nulle pour le client hébergé.

   Activé (autoriser)

   Écrit un avertissement dans le journal mais autorise l'archivage, lorsqu'un objet avec client hébergé obligatoire est créé ou mis à jour avec une valeur nulle pour le client hébergé.

8. Cliquez Sur Enregistrer, puis sur Actualiser.

   La page affiche vos modifications.

9. Fermez la fenêtre.

   La page Liste des options s'affiche à nouveau.

10. Redémarrez les services.

    L'hébergement multiclient est entièrement fonctionnel.

Vérification de la mise en oeuvre et résolution des problèmes

Vérifiez la mise en oeuvre et résolvez les éventuels problèmes.

1. Connectez-vous à CA SDM avec le nom d'utilisateur à forts privilèges (généralement ServiceDesk).
2. Cliquez sur l'onglet Administration et accédez à la liste des clients hébergés.

   Le fournisseur indique Oui pour l'utilisateur à forts privilèges dans le champ du nom du client hébergé.

3. Vérifiez que vos restrictions d'hébergement multiclient sont appliquées en recherchant une liste de contacts.

   Si les tables avec client hébergé obligatoire incluent des données sans client hébergé dans un système d'hébergement multiclient, le message suivant s'affiche dans la liste des contacts :

   `AHD05358 nn objets de contact activés sans client hébergé ont été détectés au démarrage de CA Service Desk Manager.`

Important : Si la base de données contient des données sans client hébergé, vous pouvez définir l'option d'hébergement multiclient sur Activé (avertissement) ou Activé (autoriser). Ces modes permettent de mettre à jour des tables avec client hébergé obligatoire mais affichant une valeur nulle pour le client hébergé. Cette méthode évite de perdre des données lorsqu'un accord sur les niveaux de service (SLA) ou l'événement associé est exécuté pour un billet qui n'inclut aucun client hébergé.

4. (Facultatif) Désactivez l'hébergement multiclient si des problèmes surviennent et effectuez les opérations suivantes :
   a. Restaurez les tables Domain_Constraint et usp_role.
   b. Définissez l'option Hébergement multiclient en mode de configuration.
   c. Redémarrez le système.

   Le site peut reprendre les opérations précédentes pendant que vous corrigez les problèmes ayant nécessité la restauration.

Activez Multi-Tenancy

Lorsque vous utilisez le produit, vous pouvez activer l'hébergement multiclient.

Pour activer l'hébergement multiclient

1. Cliquez sur l'onglet Administration.
2. Dans l'arborescence à gauche, cliquez sur Gestionnaire d'options, Hébergement multiclient.

   La page Liste des options s'affiche.
3. Cliquez sur Hébergement multiclient.

   La page Détail des options de l'hébergement multiclient apparaît.
4. Cliquez sur Modifier.

   La page Mettre à jour les options s'affiche.
5. Dans la liste déroulante Valeur de l'option, sélectionnez l'*une* des options suivantes :

   désactivé

   Désactive la fonction d'hébergement multiclient.

   installation

   Permet l'hébergement multiclient en mode de configuration. Dans ce mode, CA SDM affiche les objets et attributs associés aux clients hébergés modifiables pour les administrateurs des fournisseurs de services, mais n'applique pas les exigences d'hébergement. D'autres utilisateurs peuvent continuer à travailler comme si l'hébergement multiclient n'était pas installé.

activé

Active la fonction d'hébergement multiclient qui devient entièrement opérationnelle. Vous pouvez sélectionner les valeurs suivantes :

- **strict** (valeur par défaut) : CA SDM fait échouer un archivage dans une table avec client hébergé obligatoire lorsque le client hébergé est nul et que le produit ne peut pas le prendre par défaut d'un SREL à une table avec client hébergé.
- **avertir** : CA SDM écrit une erreur dans le journal, mais autorise l'archivage lorsqu'un objet associé à un client hébergé avec un client hébergé nul est créé ou mis à jour.
- **autoriser** : CA SDM écrit un avertissement dans le journal, mais autorise l'archivage lorsqu'un objet associé à un client hébergé avec un client hébergé nul est créé ou mis à jour.

Remarque : Si vous n'avez pas rempli la table ca_tenant, vous devez sélectionner Configuration dans la liste déroulante Valeur de l'option. Pour de nouvelles mises en oeuvre d'hébergement multiclient, sélectionnez Configuration.

6. Cliquez sur Installer.

   L'option Hébergement multiclient est maintenant installée.

7. Cliquez sur Actualiser.

   La page affiche vos modifications.

8. Fermez la fenêtre.

   La page Liste des options s'affiche à nouveau.

9. Redémarrez les services.

Initialisation d'un nouveau client hébergé

En tant que fournisseur de services, il se peut que vous souhaitiez créer un ensemble de données standard pour un nouveau client hébergé, comme les catégories, les partitions de données, les modèles de ticket, etc. Pour ce faire, vous pouvez utiliser pdm_extract ou pdm_tenant_extract pour créer un fichier d'entrée pdm_userload contenant les données souhaitée.

Si nécessaire, vous pouvez modifier ce fichier avec un éditeur de texte. Il peut puis être chargé dans la base de données à l'aide de pdm_userload avec l'argument -t qui définit la colonne de client hébergé sur le nouveau client hébergé. Pour plus d'informations sur les arguments pdm_userload autres que -t, reportez-vous au *Manuel d'administration*.

Le processus suivant décrit comment initialiser un nouveau client hébergé :

1. Créez le client hébergé dans la table ca_tenant.

   Utilisez la page en ligne Créer un client hébergé (page 327).

2. Chargez les données standard comme décrit plus haut.

   Utilisez pdm_userload -t pour définir le client hébergé.

3. Créez des enregistrements de contact pour le nouveau client hébergé.

   Chargez les données externes ou utilisez pdm_userload -t.

Conversion d'une mise en oeuvre de client hébergé existante en objet de client hébergé

Vous avez peut-être utilisé des partitions de données et un autre objet CA SDM pour obtenir la fonctionnalité désormais fournie par l'hébergement multiclient. Si vous voulez convertir une mise en oeuvre en hébergement multiclient, la première étape consiste à mapper les données de l'objet utilisé antérieurement au nouvel objet de client hébergé. L'objet utilisé antérieurement est appelé objet *pré-client hébergé*. Pour la plupart des sites ayant ces exigences, l'objet org (organisation) est l'objet pré-client hébergé, mais l'approche suivante peut être utilisée pour tout objet pré-client hébergé.

1. Si l'objet de pré-client hébergé n'est pas org, vérifiez que sa définition d'objet Majic spécifie TENANT_REQUIRED.

2. Vérifiez les mappages d'attribut du pré-client hébergé vers le nouvel objet de client hébergé dans le fichier buildtenant.xml à l'emplacement suivant :

   $NX_ROOT/samples/multi_tenancy

   Remarque : Vous devez copier le fichier buildtenant.xml dans le répertoire $NX_ROOT/site/cfg. De plus, buildtenant.xsd doit être dans le même répertoire que buildtenant.xml, ou vous recevrez un message d'erreur. Lorsque vous installez le produit, buildtenant.xsd est situé dans $NX_ROOT/site/cfg, donc vous n'avez pas à copier ce fichier.

   Les paramètres par défaut sont basés sur org. Si l'objet de pré-client hébergé n'est pas org, vous devez modifier le fichier.

3. Exécutez pdm_buildtenant -f (page 334).

   Un nouveau client hébergé est créé pour chaque objet de pré-client hébergé, et définit l'attribut de client hébergé dans l'objet de pré-client hébergé pour référencer le nouveau client hébergé.

4. Connectez-vous à CA SDM et vérifiez l'objet de client hébergé ainsi que l'objet de pré-client hébergé.

   Remarque : Dans certaines situations, il se peut que vous deviez mapper plusieurs objets pré-clients hébergés à un seul objet de client hébergé. Pour ce faire, actualisez manuellement les objets de pré-clients hébergés concernés et supprimez ou désactivez les clients hébergés inutilisés.

Remplissage des attributs de client hébergé dans vos tables

Pour remplir l'attribut de client hébergé dans tout ou partie d'une table, utilisez l'utilitaire *pdm_settenant*. Cet utilitaire utilise un fichier de configuration pour sélectionner les objets qui doivent devenir des clients hébergés et pour spécifier où obtenir le client hébergé pour les objets. Vous pouvez spécifier un client hébergé explicite ou indiquer que le client hébergé doit être dérivé d'une référence SREL dans l'objet devant devenir client hébergé.

Pour remplir les attributs de client hébergé dans vos tables à l'aide de pdm_settenant, effectuez les opérations suivantes :

1. Créez ou modifiez un fichier de configuration.

   Le fichier de configuration sélectionne les lignes dont l'attribut de client hébergé sera défini et spécifie une source pour la valeur de l'attribut de client hébergé. Le produit fournit un exemple de fichier settenant.xml à l'emplacement suivant :

   $NX_ROOT/samples/multi_tenancy

   Remarque : Vous pouvez modifier l'exemple de fichier settenant.xml ou créer un fichier et le copier dans le répertoire $NX_ROOT/site/cfg. De plus, settenant.xsd doit être dans le même répertoire que settenant.xml, ou vous recevrez un message d'erreur. Lorsque vous installez le produit, settenant.xsd est situé dans $NX_ROOT/site/cfg, donc vous n'avez pas à copier ce fichier.

2. Exécutez pdm_ settenant -f [fichier de configuration] -r (page 336)

   L'utilitaire pdm_settenant lit son fichier de configuration et traite chaque règle qu'il définit l'une après l'autre.

   Nous vous recommandons d'utiliser cet utilitaire d'abord pour remplir l'attribut de client hébergé dans l'objet cnt (contact), puis d'utiliser l'objet cnt comme source pour remplir le client hébergé dans les autres objets.

   Lorsque l'objet cnt est correctement devenu un client hébergé, il peut être utilisé comme base pour définir le client hébergé dans d'autres tables en exécutant les opérations suivantes :

   a. Spécifiez une règle de client hébergé avec type="SREL" dans le fichier de configuration pour un attribut référençant l'objet cnt pour définir le client hébergé dans d'autres tables.

   b. (Facultatif) Spécifiez une règle de client hébergé avec type="Name" < tenantname > pour définir le client hébergé dans certaines des tables.

3. Exécutez pdm_settenant avec un nouveau fichier de configuration.

4. Exécutez pdm_settenant à nouveau le cas échéant.

   Après avoir rempli la colonne de client hébergé dans un objet, vous pouvez utiliser les SREL pour cet objet comme base d'une règle de client hébergé SREL pour définir le client hébergé dans d'autres objets.

Exemple : Syntaxe de type SREL

La syntaxe de type SREL recherche les objets cnt dontla valeur de client hébergé n'est pas spécifiée et utilise la valeur de client hébergé de l'objet d'organisation lié :

```
<Object name="cnt">
<TenantRule type="Name">SREL</TenantRule>
<Where>client hébergé est null</Where>
</Object>
```

Exemple : Syntaxe de type de nom

La syntaxe de type de nom vérifie les objets org dont la valeur de client hébergé n'est pas spécifiée et définit leur champ de client hébergé sur le nom d'un objet de client hébergé réel :

```
<Object name="org">
<TenantRule type="Name">Tenant A</TenantRule>
<Where>client hébergé est null</Where>
</Object>
```

Créer un Client Hébergé

Vous pouvez utiliser le produit pour créer un groupe de client hébergé.

Pour créer un groupe de clients hébergés

1. Sélectionnez Gestion des rôles et de la sécurité, Clients hébergés sous l'onglet Administration.

   La page Liste de clients hébergés s'affiche.

   Remarque : L'option Clients hébergés dans Gestion des rôles et de la sécurité n'est disponible que lorsque l'hébergement multiclient est installé (activé ou configuré).

2. Cliquez sur Créer.

   La page Créer un client hébergé s'affiche.

3. Renseignez les champs modifiables si nécessaire :

   Nom

   Affiche le nom du client hébergé.

   Fournisseur de services

   Identifie si un client hébergé est le fournisseur de services. Le premier client hébergé créé est toujours le Fournisseur de Services.

   Numéro du client hébergé

   (À titre d'information uniquement) Affiche le numéro du client hébergé. Ce champ n'est pas utilisé par CA SDM.

État de l'enregistrement

Configure le client hébergé sur Activé ou Désactivé.

Client hébergé parent

Spécifie un autre client hébergé au-dessus de ce client hébergé, en faisant de ce dernier un *client hébergé fils* dans une hiérarchie de clients hébergés.

Clients hébergés fils autorisés

Permet à ce client hébergé d'avoir des clients hébergés fils. Le client hébergé ne peut pas modifier le paramètre.

Profondeur du client hébergé

(À titre d'information uniquement) Indique la profondeur de ce client hébergé.

Groupe de clients hébergés pères

(À titre d'information uniquement) Identifie le groupe de clients hébergés géré par le système et qui contient ce client hébergé et tous les clients hébergés qui lui sont supérieurs dans la hiérarchie.

Groupe de clients hébergés fils

(À titre d'information uniquement) Identifie le groupe de clients hébergés géré par le système et qui contient ce client hébergé et tous les clients hébergés qui lui sont inférieurs dans la hiérarchie.

Groupe de clés étrangères

(À titre d'information uniquement) Identifie le groupe de clients hébergés géré par le système et qui contient des clients hébergés pouvant être référencés à partir d'une SREL dans des données qui appartiennent à ce client hébergé. Le groupe de clés étrangères est identique au groupe de clients hébergés pères.

Groupe de clients hébergés associés

(À titre d'information uniquement) Identifie le groupe de clients hébergés géré par le système et qui comprend aussi bien des groupes de clients hébergés pères que des groupes de clients hébergés fils pour ce client hébergé.

Conditions d'utilisation

Spécifie les conditions d'utilisation pour le client hébergé.

Logo

Spécifie l'adresse URL du fichier de logo du client hébergé, qui peut être un type quelconque d'image Web.

Emplacement

Affiche la page de recherche de sites.

Contact

Affiche la page de recherche de contacts.

Remarque : Si aucun contact n'est associé au client hébergé respectif, les champs Adresse de courriel et Adresse de courriel du téléavertisseur sont désactivés.

4. Cliquez sur Enregistrer.

   Le client hébergé est créé.

5. Fermez la fenêtre.

6. Cliquez avec le bouton droit de la souris sur Liste de clients hébergés et sélectionnez Actualiser.

   La Liste des clients hébergés est actualisée et affiche le client hébergé créé.

7. (Facultatif) Pour affecter ce client hébergé à des groupes de clients hébergés définis par l'utilisateur, cliquez sur Mettre à jour les groupes de clients hébergés dans l'onglet Groupes de clients hébergés.

Créer un groupe de clients hébergés

Vous pouvez utiliser le produit pour créer un groupe de client hébergé.

Pour créer un groupe de clients hébergés

1. Dans l'onglet Administration, sélectionnez Gestion des rôles et de sécurité.

2. Cliquez sur Groupes de clients hébergés.

   La liste des groupes de clients hébergés s'affiche.

   Remarque : L'option Groupes de clients hébergés dans Gestion des rôles et de la sécurité est disponible uniquement lorsque l'hébergement multiclient est installé (activé ou configuré).

3. Cliquez sur Créer.

   La page Créer un groupe de clients hébergés s'affiche.

4. Remplissez les champs suivants :

   Nom du groupe de clients hébergés

   Affiche le nom du groupe de clients hébergés sélectionné.

   État de l'enregistrement

   Définit le groupe de clients hébergés comme activé ou désactivé

   Description

   Affiche une description du groupe de clients hébergés.

5. Cliquez sur Enregistrer.

   Le groupe de clients hébergés est créé.

6. Fermez la fenêtre.

   La liste des groupes de clients hébergés s'affiche.

7. Cliquez avec le bouton droit de la souris sur Liste de clients hébergés et sélectionnez Actualiser.

   La liste des groupes de clients hébergés est mise à jour.

8. Cliquez sur Mettre à jour les clients hébergés sur la page Détails du groupe de clients hébergés pour ajouter des membres de client hébergé au groupe.

Hiérarchies des clients hébergés

Une *hiérarchie des clients hébergés* est un groupe de clients hébergés structuré qui est créé par le système ou modifié lorsque vous affectez un *client hébergé parent* à un client hébergé. Le client hébergé devient un *client hébergé fils* des clients hébergés parents et supérieurs (le cas échéant) dans cette hiérarchie.

Remarque : Le fournisseur de services peut créer de multiples hiérarchies non associées ou n'en créer aucune. Même dans un système avec des hiérarchies de clients hébergés, vous pouvez définir des clients hébergés autonomes.

Un client hébergé fils représente généralement une subdivision à l'intérieur de ses *clients hébergés pères*. Un client hébergé fils peut avoir ses propres règles et données commerciales, et les données du client hébergé père sont "transférées" automatiquement vers le client hébergé fils en lecture seule.

CA SDM prend en charge une hiérarchie de clients hébergés de profondeur illimitée. Toutefois, le *fournisseur de services* peut spécifier une limite sur le nombre total de clients hébergés et la profondeur des hiérarchies de clients hébergés (la limite par défaut est de quatre niveaux). Le fournisseur de services détermine aussi si des clients hébergés spécifiques peuvent avoir des clients hébergés fils.

Remarque : Le fournisseur de services peut participer à des hiérarchies de clients hébergés, mais cela n'est pas obligatoire. Le fournisseur de services ne peut pas avoir de client hébergé parent.

Création d'un client hébergé fils

L'hébergement de client fils permet de construire et de modifier des hiérarchies de clients hébergés à des fins organisationnelles et de partage de données. Pour mettre un client hébergé dans une hiérarchie de clients hébergés, vous lui affectez un client hébergé parent.

Créer un client hébergé fils :

1. Sous l'onglet Administration, sélectionnez Gestion des rôles et de la sécurité, Clients hébergés.

   La liste des clients hébergés s'affiche.

   Remarque : L'option Clients Hébergés dans Gestion des rôles et de la sécurité est disponible uniquement lorsque l'hébergement multiclient est activé.

2. Cliquez sur un client hébergé existant à modifier, ou cliquez sur Créer.

   La page Détails du client hébergé apparaît. Entrez toute donnée ou tout changement requis.

3. Sélectionnez un client hébergé parent.

   Remarque : La liste déroulante Client hébergé parent affiche uniquement les clients hébergés qui ont l'autorisation d'avoir des clients hébergés fils.

4. Cliquez sur Enregistrer.

   Le client hébergé est un client hébergé fils du client hébergé parent.

   Remarque : Si un client hébergé est un client hébergé fils, il appartient au groupe de clients hébergés fils du client hébergé parent, tout comme les éventuels clients hébergés fils de ce client hébergé fils, etc. Le client hébergé parent rejoint le groupe de clients hébergés pères du client hébergé fils, tout comme les éventuels clients hébergés pères de ce client hébergé père, etc. Chacun joint le groupe des clients hébergés associés de l'autre.

Groupes de clients hébergés gérés par le système

CA SDM génère et gère automatiquement trois groupes de clients hébergés pour chaque client hébergé dans une hiérarchie de clients hébergés (*client hébergé* est le nom du client hébergé) :

- *client-hébergé*_clients-hébergés-fils (client hébergé, ses clients hébergés enfants et leurs clients hébergés fils inférieurs)
- *client-hébergé*_clients-hébergés-pères (client hébergé, son client hébergé parent et ses clients hébergés pères supérieurs)
- *client-hébergé*_clients-hébergés-associés (hiérarchie complète unique)

Les groupes de clients hébergés gérés par le système peuvent être utilisés comme des groupes de clients hébergés définis par l'utilisateur. Néanmoins seuls leurs noms et leurs descriptions peuvent être modifiés.

Exportation et importation des données du client hébergé

Le fournisseur de services peut extraire des données de client hébergé à partir d'une mise en oeuvre d'hébergement multiclient existante et les importer dans un nouveau système.

Remarque : Selon le volume de vos données, le processus d'extraction peut prendre plusieurs heures. Il se peut que vous deviez effectuer l'extraction et l'importation en plusieurs phases, comme suit :

Initial

Extrait une ligne de base et crée un fichier de contrôle utilisé dans des phases ultérieures.

Mettre à jour

Utilise le fichier de contrôle pour extraire uniquement les données qui ont été modifiées depuis l'exécution précédente.

Final

Effectue les mêmes étapes que la mise à jour, sauf que les animations sont aussi extraites. Les animations sont omises dans les phases initiale et de mise à jour.

Pour extraire des données à partir d'une base de données et les importer dans un autre, effectuez les opérations suivantes :

1. Exécutez une phase initiale de pdm_tenant_extract (page 340) pour extraire les données de référence. Le fichier de contrôle utilisé dans les phases ultérieures est ainsi créé.
2. Préparez une nouvelle MDB pour les données extraites.

   Important : Le résultat de la phase initiale *doit* être chargé dans une base de données qui n'a jamais été utilisée avec ce produit, ni aucun autre produit. Chaque table chargée à partir des données de phase initiales est tronquée avant le chargement, ce qui pourrait causer la perte de données si la base de données est déjà utilisée.
3. Pour éviter l'apparition des doublons de contacts privilégiés sur le nouveau système, vous devez désactiver les contacts privilégiés. Connectez-vous à CA SDM et définissez l'état de ces contacts sur Désactivé avant de charger les données extraites.
4. Pour éviter des problèmes référentiels pendant le chargement des données, exécutez le script de contraintes de dépôt approprié :
   - (Oracle) Exécutez $NX_ROOT/samples/views/Oracle/OracleDropConstraints.sql
   - (SQL Server) Exécutez $NX_ROOT/samples/views/SQLServer/SQLDropConstraints.sql
5. Utilisez pdm_userload (page 341) pour charger les données de la phase initiale dans la nouvelle MDB préparée aux étapes 2 et 3.
6. Exécutez une mise à jour ou dernière phase de pdm_tenant_extract pour extraire les données supplémentaires créées ou modifiées depuis la phase précédente. Pdm_tenant_extract utilise le fichier de contrôle créé à l'étape 1 pour déterminer les données déjà traitées par la phase précédente.
7. Utilisez pdm_userload pour charger les données extraites à l'étape 5 dans la même MDB contenant les données chargées aux phases précédentes.

   Remarque : Pour plus d'informations sur cet utilitaire, reportez-vous à pdm_userload (page 341).

8. Répétez les étapes 5 et 6 si nécessaire jusqu'à ce que toutes les données aient été importées dans la nouvelle base de données. La dernière exécution doit correspondre à la dernière phase.
9. Pour protéger l'intégrité de la nouvelle base de données, restaurez les contraintes déposées à l'étape 3 en exécutant le script d'ajout de contraintes approprié :
   - (Oracle) Exécutez $NX_ROOT/samples/views/Oracle/OracleAddConstraints.sql
   - (SQL Server) Exécutez $NX_ROOT/samples/views/SQLServer/SQLAddConstraints.sql
10. Utilisez pdm_tenant_delete (page 339) pour supprimer les données extraites de la base de données d'origine.
11. Assurez-vous que tous les référentiels associés aux clients hébergés extraits sont copiés vers les paramètres cibles.

Traitement des pièces jointes et des référentiels

Les pièces jointes sont stockées dans des référentiels. Vous devez copier tous les référentiels qui sont associés aux clients hébergés extraits vers le système cible, y compris les référentiels publics. Ce processus est essentiellement une opération manuelle, composée des étapes suivantes :

1. Redéfinissez les informations spécifiques à l'emplacement pour tous les référentiels, après l'achèvement du chargement initial des données dans le système cible. Cette tâche inclut la modification des valeurs suivantes :
   - Nom du serveur
   - Chemin de téléchargement
   - Chemin d’accès au servlet
   - Chemin d’archivage
2. Ccréez manuellement tous les répertoires et les dossiers obligatoires.
3. Copiez toutes les pièces jointes de l'emplacement précédent vers le nouvel emplacement du référentiel après (ou pendant) le chargement des données lors de la phase finale.

Après avoir terminé cette procédure, toutes les références aux pièces jointes dans le système cible doivent réussir. Pourtant, des copies des pièces jointes restent sur le système source. Utilisez l'utilitaire pdm_clean_attachments.pl (page 336) pour nettoyer ces pièces jointes redondantes.

Utilitaires utilisés pour l'hébergement multiclient.

Cette section décrit les utilitaires qui sont utilisés pour gérer un environnement d'hébergement multiclient.

Remarque : Les paramètres obligatoires sont entre "{ }" et les paramètres facultatifs entre "[ ]".

Renseignements supplémentaires :

pdm_buildtenant : Création de clients hébergés à partir d'un autre objet (page 334)
pdm_clean_attachments—Suppression des pièces jointes redondantes après l'importation des données de client hébergé (page 336)
pdm_settenant : Affectation de clients hébergés aux objets (page 336)
pdm_tenant_delete—Suppression de données de client hébergé dans une base de données (page 339)
pdm_tenant_extract—Extraction des données du client hébergé (page 340)
pdm_userload—Chargement de données de client hébergé (page 341)

pdm_buildtenant : Création de clients hébergés à partir d'un autre objet

L'utilitaire *pdm_buildtenant* est utilisé pour créer des clients hébergés à partir d'un autre objet. Vous avez peut-être utilisé des partitions de données et un autre objet CA SDM pour obtenir la fonctionnalité désormais fournie par l'hébergement multiclient. Si vous souhaitez convertir une mise en oeuvre en hébergement multiclient, la première étape consiste à utiliser pdm_buildtenant pour mapper les données de l'objet utilisé auparavant au nouvel objet de client hébergé.

Important : Avant d'exécuter pdm_buildtenant, vous *devez* configurer le fournisseur de services.

Dans cette section, l'objet utilisé pour recevoir les informations de type client hébergé est appelé objet de pré-client hébergé. Pour la plupart des sites ayant ces exigences, l'objet org (organisation) est l'objet pré-client hébergé, mais l'approche suivante peut être utilisée pour tout objet pré-client hébergé.

L'utilitaire pdm_buildtenant crée les objets de client hébergé à partir des objets pré-client hébergé. L'application crée un nouveau client hébergé pour chaque objet pré-client hébergé et définit l'attribut du client hébergé dans l'objet pré-client hébergé pour référencer le nouveau client hébergé. L'utilitaire a la syntaxe suivante :

```
pdm_buildtenant [-h] | [-f [fichier_de_configuration]
```

-f configuration_file

(Facultatif) Spécifie l'emplacement d'un fichier de configuration spécifiant les règles de création de clients hébergés à partir de l'objet pré-client hébergé. Si cet argument n'est pas inclus, pdm_buildtenant utilise le fichier de configuration du répertoire $NX_ROOT/site/cfg. Ce fichier suppose que l'objet pré-client hébergé est org ; si ce n'est pas le cas, vous *devez* modifier le fichier de configuration avant d'utiliser pdm_buildtenant.

Remarque : Vous *devez* copier le fichier buildtenant.xml dans le répertoire $NX_ROOT/site/cfg. De plus, buildtenant.xsd doit être dans le même répertoire que buildtenant.xml, ou vous recevrez un message d'erreur. Lorsque vous installez le produit, buildtenant.xsd est situé dans $NX_ROOT/site/cfg, donc vous n'avez pas à copier ce fichier.

-h

Affiche les informations d'utilisation pour pdm_buildtenant.

Le format suivant est le format du fichier de configuration.

```
<?xml version="1.0" encoding="utf-8" ?>
<BuildTenant>
    <Object from="MajicObjectName">
        <Attribute from="sourceAttribute1" to="tenantAttribute1" />
        <Attribute from="sourceAttribute2" to="tenantAttribute2" />
    </Object>
</BuildTenant>
```

L'attribut *from* de la balise Object identifie l'objet pré-client hébergé. Chaque balise Attribute identifie un attribut qui doit être copié depuis l'objet pré-client hébergé vers un attribut du nouveau client hébergé.

Important : Pour les mises en oeuvre d'hébergement multiclient sous UNIX, vous *devez* exécuter pdm_task pour exporter LIBPATH avant d'exécuter les utilitaires pdm_settenant et pdm_buildtenant. Si vous n'exécutez pas pdm_task avant d'exécuter ces utilitaires, vous recevrez des messages d'erreurs système. Utilisez ../pdm_task pour exécuter la commande.

pdm_clean_attachments—Suppression des pièces jointes redondantes après l'importation des données de client hébergé

Après l'importation des données de client hébergé, vous devez supprimer les pièces jointes redondantes. L'utilitaire a la syntaxe suivante :

```
pdm_perl pdm_clean_attachments.pl [-h] | [-n repository_name] | [-S|-K]
```

-h

Spécifie d'afficher l'aide de ligne de commande.

-n *repository_name*

Spécifie le nom de la version du référentiel à traiter S'il n'est pas spécifié, tous les référentiels sont traités.

-S

Spécifie que seuls les référentiels de CA SDM sont traités.

-K

Spécifie que seuls les référentiels de Gestion des connaissances et les référentiels avec images incorporées sont traités.

Remarque : L'exécution de la commande pdm_clean_attachments.pl sans arguments traite tous les référentiels.

Important : Sous UNIX, la valeur LIBPATH doit être définie avant d'exécuter plusieurs utilitaires CA SDM. Utilisez *pdm_task* pour définir la valeur LIBPATH avant l'exécution d'un utilitaire. Par exemple, entrez "pdm_task pdm_clean_attachments ...".

pdm_settenant : Affectation de clients hébergés aux objets

Après avoir défini des clients hébergés, vous devez utiliser l'utilitaire *pdm_settenant* pour définir la colonne de clients hébergés dans d'autres objets. L'utilitaire a la syntaxe suivante :

```
pdm_settentant [-h] | {-f [configuration_file] | -r} [-d domsrvr]
```

-d domsrvr

(Facultatif) Spécifie un domsrvr à utiliser. Si cet argument n'est pas spécifié, pdm_settenant utilise le domsrvr par défaut.

-f *configuration_file*

(Facultatif) Indique l'emplacement d'un fichier de configuration spécifiant les données qui seront mises à jour et les règles de mise à jour du fichier. Si cet argument n'est pas spécifié, pdm_settenant utilise le fichier de configuration du répertoire $NX_ROOT/site/cfg (une fois que le fichier de configuration est copié dans le dossier $NX_ROOT/site/cfg).

Remarque : Vous pouvez modifier l'exemple de fichier settenant.xml ou créer un fichier et le copier dans le répertoire $NX_ROOT/site/cfg. De plus, settenant.xsd doit être dans le même répertoire que settenant.xml, ou vous recevrez un message d'erreur. Lorsque vous installez le produit, settenant.xsd est situé dans $NX_ROOT/site/cfg, donc vous n'avez pas à copier ce fichier.

L'exemple de code XML suivant décrit le format de ce fichier :

```
<?xml version="1.0" encoding="utf-8" ?>
<SetTenant>
    <Object name="MajicObjectName">
        <TenantRule type="SREL">MajicColumName</TenantRule>
        <Where>client hébergé est null</Where>
    </Object>
    <Object name="MajicObjectName">
    <TenantRule type="Name">TenantName</TenantRule>
    <Where>client hébergé est null</Where>
    </Object>
</SetTenant>
```

Chaque balise d'objet spécifie un objet CA SDM devant devenir client hébergé. La balise TenantRule spécifie comment pdm_settenant doit déterminer le client hébergé, et la balise Where sélectionne les objets devant devenir clients hébergés. Il existe deux types de balises TenantRule :

- type="Name"

  Spécifie un client hébergé explicite par nom.

- type="SREL"

  Spécifie un attribut SREL dans l'objet. Pdm_settenant copie le client hébergé de l'objet référencé par SREL.

-h

Affiche les informations d'utilisation de pdm_settenant.

-r

Sort un rapport affichant le nombre total de lignes dans chaque table qui requiert un client hébergé et le nombre de lignes ayant une colonne de client hébergé nulle.

Remarque : Si les deux arguments -f et -r sont spécifiés, pdm_settenant sort un rapport après avoir terminé sa mise à jour. Si vous spécifiez uniquement l'argument -r, pdm_settenant sort un rapport, mais n'actualise aucune donnée.

L'exécution de pdm_settenant sans aucun argument affiche les informations d'utilisation. Pour exécuter pdm_settenant à l'aide du fichier de configuration par défaut, spécifiez l'option -f sans l'argument configuration_file. L'utilitaire pdm_settenant lit son fichier de configuration et traite chaque règle qu'il définit l'une après l'autre. Il écrit la sortie dans le fichier pdm_settenant.log dans le répertoire $NX_ROOT/log.

Vous pouvez exécuter pdm_settenant autant de fois que nécessaire. La première exécution peut prendre un certain temps (jusqu'à plusieurs heures pour un grand site). Les exécutions suivantes sont plus rapides car elles traitent uniquement les lignes qui n'ont pas été mises à jour. Ceci prépare la base de données avant l'installation de l'option d'hébergement multiclient.

Important : Pour les mise en oeuvre d'hébergement multiclient sous UNIX, vous devez exécuter pdm_task pour exporter LIBPATH avant d'exécuter les utilitaires pdm_settenant et pdm_buildtenant. Si vous n'exécutez pas pdm_task avant d'exécuter ces utilitaires, vous recevrez des messages d'erreurs système. Utilisez ../pdm_task pour exécuter la commande.

Considérations d'affectation des clients hébergés aux objets

Après avoir défini des clients hébergés, vous devez utiliser l'utilitaire pdm_settenant (affectation de clients hébergés aux objets) pour définir la colonne Client hébergé dans les autres objets. Lorsque vous modifiez le client hébergé pour un objet, vous devez considérer la possibilité de modifier l'hébergement sur les objets avec client hébergé associés afin de maintenir l'intégrité des données. La non-synchronisation de ces objets peut provoquer l'absence de données de CI, relations, DRG, version, etc. Les objets CA CMDB suivants ont un client hébergé :

- nr : définitions d'éléments de configuration
- nr_com : entrées de journal associées à un CI
- bmhier : relations associées à des CI
- mdr_idmap : définitions de fournisseur RDG
- ci_mdr_idmap : mappages fédérés CI/RDG

Pour chaque CI, effectuez les opérations suivantes pour synchroniser les données lorsque vous utilisez pdm_settenant pour modifier l'hébergement :

- Spécifiez nr comme nom de l'objet de CI.
- Modifiez les entrées de journal associées au CI dans nr_com pour que vous puissiez afficher les entrées de journal pour le nouveau client hébergé.

Remarque : Pour plus d'informations sur la commande pdm_settenant, reportez-vous au *Manuel d'administration*.

Exemple : XML pour modifier le client hébergé et le journal

Le XML suivant modifie le client hébergé pour un CI nommé CITest dans T2 et modifie également les entrées de journal correspondantes dans nr_com :

```
<TenantRule type="Name">T2</TenantRule>
<Where>name = 'CITest'</Where>
</Object>
<Object name="nr_com">
<TenantRule type="Name">T2</TenantRule>
<Where>asset_id.name = 'CITest'</Where>
\</Object>
```

pdm_tenant_delete—Suppression de données de client hébergé dans une base de données

L'utilitaire *pdm_tenant_delete* supprime de la base de données toutes les données d'un client hébergé spécifié.

Important : Les contraintes référentielles de ca_tables doivent être déposées avant l'exécution de pdm_tenant_delete et être restaurées ensuite.

L'utilitaire a la syntaxe suivante :

```
pdm_tenant_delete -h|-t tenant_name [-C|-R] [-Q]
```

-h

Affiche les informations d'utilisation de pdm_tenant_delete.

-t *tenant_name*

Spécifie le nom du client hébergé des données à supprimer.

Remarque : Le client hébergé doit être marqué comme inactif pour que vous puissiez utiliser cet utilitaire pour supprimer les données.

-C

Spécifie que tous les contacts d'un client hébergé seront marqués comme inactifs. Puisque les contacts peuvent être partagés entre les produits, la logique par défaut ne doit pas supprimer ou désactiver des contacts en série, sauf en cas de demande explicite.

Remarque : Cette option est ignorée si l'option -R est spécifiée.

-R

Spécifie que toutes les lignes de toutes les tables avec client hébergé marquées comme CA_COMMON en ddict.sch seront supprimées, y compris l'objet de client hébergé lui-même.

Important : Ces tables sont partagées entre plusieurs produits, utilisez donc cette option avec prudence.

-Q

Spécifie un traitement de requête rapide pour exécuter aussi rapidement que possible des requêtes de base de données. Si cet argument n'est pas spécifié, l'utilitaire utilise le traitement de requête d'arrière-plan pour que les requêtes s'exécutent uniquement quand le système est inactif. Cet argument s'améliore le temps d'exécution au détriment d'un impact plus élevé sur un système actif.

Important : Sous UNIX, la valeur LIBPATH doit être définie avant d'exécuter plusieurs utilitaires CA SDM. Utilisez *pdm_task* pour définir la valeur LIBPATH avant l'exécution d'un utilitaire. Par exemple, entrez "pdm_task pdm_clean_attachments ...".

pdm_tenant_extract—Extraction des données du client hébergé

L'utilitaire *pdm_tenant_extract* extrait de la base de données toutes les données d'un client hébergé spécifié. Il extrait les données au format pdm_userload pour qu'elles puissent être facilement chargées dans une autre base de données. L'utilitaire a la syntaxe suivante :

```
pdm_tenant_extract -h | -c control_file [-d domsrvr] [-g yes|no] [-o output_file]
        -p phase  [[-t tenant_name]…] [-Q] [table1 [table2...]]
```

-h

Affiche les informations d'utilisation de pdm_tenant_extract.

-c *control_file*

Spécifie l'emplacement du fichier de contrôle pour cet extrait de client hébergé. Pendant la phase initiale, le fichier est créé à l'emplacement spécifié (et il ne doit pas déjà exister). Le fichier doit exister pour les phases de mise à jour et finale.

-d domsrvr

(Facultatif) Spécifie un domsrvr à utiliser.

-g yes|no

(Facultatif) Spécifie si les données publiques sont incluses ou non dans le fichier de sortie. Si cet argument n'est pas spécifié, les données publiques de toutes les tables sont incluses.

-o *output_file*

(Facultatif) Spécifie l'emplacement du fichier de sortie. Si cet argument n'est pas spécifié, la sortie est dirigée vers stdout.

-p *phase*

Spécifie la phase de l'extrait. Utilisez l'une des valeurs suivantes :

I : initiale

U : mise à jour

F : finale

-t *tenant_name*

Spécifie le nom d'un client hébergé à extraire. Cet argument est requis pendant la phase initiale et peut être répété pour plusieurs clients hébergés. Il n'est pas valide pour les phases de mise à jour et finale.

-Q

Spécifie un traitement de requête rapide pour exécuter aussi rapidement que possible des requêtes de base de données. Si cet argument n'est pas spécifié, l'utilitaire utilise le traitement de requête d'arrière-plan pour que les requêtes s'exécutent uniquement quand le système est inactif

table1 [table2...]

(Facultatif) Spécifie les tables à extraire. Si omis, toutes les tables sont extraites.

Important : La sortie de la phase initiale doit être chargée dans une base de données qui n'a jamais été utilisée avec CA SDM, ni aucun autre produit. Chaque table chargée à partir des données de phase initiales est tronquée avant le chargement, ce qui pourrait causer la perte de données si la base de données est déjà utilisée.

Remarque : Pour éviter les problèmes référentiels pendant le chargement des données, exécutez le script de suppression de contraintes approprié ($NX_ROOT/samples/views/Oracle/OracleDropConstraints.sql ou $NX_ROOT/samples/views/SQLServer/SQLDropConstraints.sql). A l'issue du chargement, appliquez les contraintes à nouveau avec le script xxxAddConstraints.sql approprié situé dans le même répertoire.

Important : Sous UNIX, la valeur LIBPATH doit être définie avant d'exécuter plusieurs utilitaires CA SDM. Utilisez *pdm_task* pour définir la valeur LIBPATH avant l'exécution d'un utilitaire. Par exemple, entrez "pdm_task pdm_clean_attachments ...".

Informations complémentaires :

Exportation et importation des données du client hébergé (page 331)

pdm_userload—Chargement de données de client hébergé

L'utilitaire *pdm_userload* sert à charger des données dans une base de données CA SDM. Cet utilitaire est disponible même si l'hébergement multiclient n'est pas installé. L'hébergement multiclient ajoute la prise en charge pour un argument supplémentaire (-t) qui spécifie le nom d'un client hébergé dont l'ID doit être inséré dans la colonne de client hébergé de toutes les lignes insérées ou mises à jour dans une table avec client hébergé. Le client hébergé spécifié doit déjà être dans la base de données.

Lors de l'extraction des données, effectuez les opérations suivantes pour éviter les erreurs dans stdlog :

1. Avant de commencer à charger des données, fermez CA SDM et redémarrez le produit en mode DBADMIN, comme suit :

   Windows

   Exécutez pdm_d_mgr -s DBADMIN

   UNIX

   Exécutez pdm_init -s DBADMIN

2. Lorsque les données sont chargées, fermez CA SDM à l'aide de la commande pdm_halt.
3. Redémarrez CA SDM en mode normal.

Remarque : Pour plus d'informations sur l'utilitaire pdm_userload, reportez-vous au *Manuel d'administration*.

Procédure d'activation du basculement automatique

La surveillance de l'intégrité du examine la façon dont un serveur réagit à la charge de fonctionnement et assure le suivi de sa réactivité aux demandes du client. Cette surveillance vise à empêcher les pannes de serveur en s'assurant que le serveur conserve toujours une capacité suffisante pour pouvoir effectuer les tâches requises. Bon nombre des outils standards de surveillance de l'intégrité prennent en charge les protocoles HTTP et HTTPS pour la surveillance à distance.

La fonctionnalité de basculement automatique CA SDM affiche les interfaces HTTP standards suivantes :

- Interface de surveillance de l'intégrité : Interface HTTP(S) utilisée pour surveiller l'intégrité du serveur d'arrière-plan. Elle prend également des décisions fiables en ce qui concerne le basculement vers un serveur de secours choisi en cas d'interruptions dans la disponibilité ou la capacité du serveur à effectuer les tâches requises.
- Interface d'initialisation du basculement : Interface HTTP(S) qui fait la promotion transparente du serveur de secours choisi comme nouveau serveur d'arrière-plan sans causer d'interruption de service.

1. Installez Apache Tomcat sur le serveur d'arrière-plan et tous les serveurs de secours.

   Remarque : Assurez-vous que Tomcat utilise JRE 1.7 et qu'il n'utilise pas le numéro de port configuré pour les composants CA SDM.

2. (Facultatif) Configurez SSL sur les serveurs Tomcat que vous avez installés. Pour de plus amples renseignements sur la configuration de SSL, reportez-vous à la section *Configuration de l'authentification SSL* ou au *Manuel d'administration*.

3. Connectez-vous au serveur d'arrière-plan.

4. Déployez le servlet d'intégrité. Effectuez les opérations suivantes :

   a. Copiez le fichier HealthServlet.war qui se trouve dans le dossier $NX_ROOT/samples/HealthServlet dans le dossier *TOMCAT_HOME*/webapps.

   b. Redémarrez Tomcat.

   Le fichier HealthServlet.war est déployé dans le dossier webapps. Pour confirmer le déploiement, assurez-vous que le dossier HealthServlet ait été créé dans le même dossier webapps.

   Une fois le déploiement réussi, le servlet d'intégrité est prêt à effectuer les vérifications d'intégrité. Cela inclut vérifier l'état de SLUMP et l'intégrité des processus CA SDM définis dans le fichier health.xml. Recherchez le fichier health.xml à l'emplacement suivant :

   TOMCAT_HOME/webapps/HealthServlet/WEB-INF/classes

5. (Facultatif) Personnalisez health.xml en fonction des besoins de votre organisation. Par exemple, vous voulez surveiller le processus du moteur Web. Utilisez la bonne balise définie dans CA SDM pour ajouter le processus dans le fichier health.xml. Effectuez les opérations suivantes pour trouver le nom de la balise :

   a. Ouvrez les fichiers pdm_startup.i et pdm_startup qui se trouvent dans le dossier $NX_ROOT/pdmconf.

   b. Cherchez, dans les deux fichiers, le processus que vous voulez surveiller.

   c. Trouvez le nom de la balise correspondante en établissant une correspondance entre les variables des deux fichiers.

Le processus webengine est ainsi défini dans le fichier pdm_startup.i :

```
#define WEBENGINE(_TAG,_HOST,_SLUMP_NAME,_DOMSRVR, _CFG, _WEBDIRECTOR,
_RPC_NAME)
```

Et comme ceci, dans pdm_startup :

```
WEBENGINE(webengine, $NX_LOCAL_HOST, web:local, domsrvr,
$NX_ROOT/bopcfg/www/web.cfg, "", "rpc_srvr:%h")
```

Cet exemple nous permet de dire que le nom de la balise du processus webengine est webengine.

Important : Si vous créez un nouveau processus, le processus actuel sera alors commenté dans le fichier updm_startup et de nouvelles entrées seront créées. Veuillez vous assurer de trouver le nom de la balise dans les entrées du nouveau processus.

Important : Si vous personnalisez health.xml, assurez-vous que le fichier XML ne comporte aucune erreur et que vous redémarrez Tomcat pour qu'il puisse refléter les modifications apportées au XML.

6. Effectuez les étapes 4 et 5 pour tous les serveurs de secours.
7. Configurez l'outil tiers choisi pour surveiller l'intégrité du serveur d'arrière-plan à intervalles réguliers. Pour surveiller l'intégrité, utilisez l'URL HTTP suivante :

   `http(s)://`*`nom_serveur_arrière-plan:numéro_port`*`/HealthServlet/GetHealth`
8. Configurez l'outil tiers afin qu'il initialise une logique de basculement lorsque l'intégrité du serveur d'arrière-plan diminue. Il est recommandé de configurer la logique de basculement pour promouvoir le serveur de secours comme nouveau serveur d'arrière-plan. Utilisez le serveur de basculement suivant dans la logique de basculement :

   Important : Il est recommandé de configurer le serveur de basculement avec SSL et de n'accorder de droits d'accès qu'aux utilisateurs prédéfinis. Cette procédure s'applique également au moment de configurer l'outil tiers d'initialisation de basculement.

   `http(s)://`*`nom_serveur_secours:numéro_port`*`/HealthServlet/FailoverServlet`

   Vous avez activé le basculement automatique.

9. Une fois la configuration terminée, l'outil tiers commencera à utiliser l'URL du servlet d'intégrité pour surveiller l'intégrité du serveur d'arrière-plan.

   - Chaque type de serveur dispose de son propre ensemble de processus. Si SLUMP et l'ensemble des autres processus CA SDM fonctionnent de façon appropriée, le serveur d'arrière-plan enverra la réponse HTTP 200 suivante, avec une charge utile prédéfinie, à l'outil tiers :

     ```
     AA-Server-Status: All OK!

     AA-Server-Role: BG
     ```

   - Si, par contre, SLUMP ou l'un des processus CA SDM (indiqués dans health.xml) arrête de fonctionner et ne peut pas reprendre, le serveur d'arrière-plan enverra la réponse HTTP 503 suivante, avec une charge utile prédéfinie, à l'outil tiers :

     ```
     AA-Server-Status: NOT OK!

     AA-Server-Role: BG
     ```

10. Si l'outil reçoit une réponse HTTP 503, il initialisera automatiquement la logique de basculement.

Chapitre 6: Personnalisation

Ce chapitre traite des sujets suivants :

Aperçu de la personnalisation (page 349)
Déplacement du module d'authentification vers un serveur externe (page 350)
Personnalisation de méthode de notification (page 357)
Personnalisation des requêtes et messages (page 366)
Personnalisation de l'interface Web (page 381)
Personnalisation du stockage des données du journal d'événements (page 497)
Personnalisation des Rapports CA Business Intelligence (page 499)
Personnalisation des rapports hérités (page 516)

Chapitre 7: Aperçu de la personnalisation

CA SDM permet d'exécuter diverses fonctions de gestion des services informatiques. Le produit fournit un large éventail de fonctions et divers contenus de bonnes pratiques pour répondre à vos besoins de gestion des services de manière aussi rapide et complète que possible.

Bien que la mise en oeuvre par défaut de CA SDM convient aux processus et à la terminologie utilisés dans la plupart des entreprises informatiques, vous pouvez moduler le produit de sorte qu'il soit en parfaite adéquation avec les spécifications de votre entreprise. Le produit inclut l'éventail d'approches suivant pour le personnaliser en fonction de vos besoins spécifiques :

- Personnalisation d'utilisateur final
- Configuration de l'ensemble du système
- Adaptation basée sur les outils
- Personnalisation au niveau du code

Il existe différents types d'approches pour personnaliser le produit.

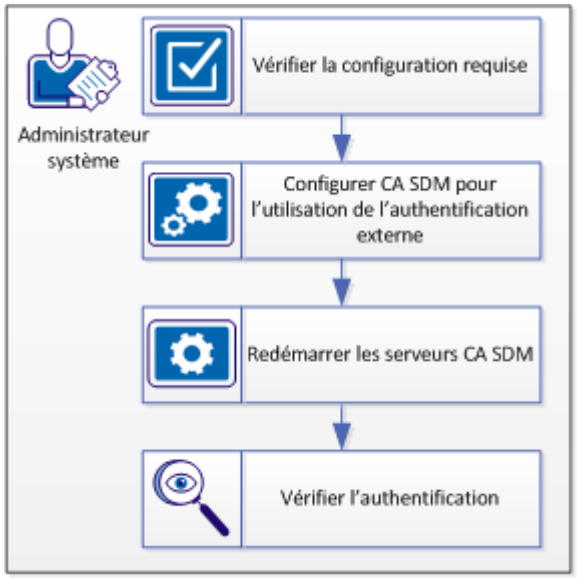
Déplacement du module d'authentification vers un serveur externe

Le module d'authentification dans CA SDM est un démon singleton responsable de l'authentification des utilisateurs. Le module d'authentification est exécuté sur le serveur principal pour la configuration conventionnelle et sur le serveur d'arrière-plan pour la configuration de disponibilité avancée. Vous pouvez déplacer le module d'authentification vers un serveur externe dans l'un des cas suivants :

- Configuration conventionnelle :
  - Le serveur principal est exécuté sur une plate-forme UNIX ou Linux et vous avez besoin d'une authentification Windows ; déplacez le module d'authentification vers un serveur secondaire Windows.
  - Le serveur principal est exécuté sur une plate-forme Solaris et vous avez besoin d'une authentification CA EEM ; déplacez le module d'authentification vers le serveur secondaire, car CA SDM ne prend pas en charge l'intégration de CA EEM sous Solaris.
- Configuration de disponibilité avancée :
  - Le serveur d'arrière-plan est exécuté sur une plate-forme UNIX ou Linux et vous avez besoin d'une authentification Windows ; déplacez le module d'authentification vers un serveur d'applications Windows.
  - Le serveur d'arrière-plan est exécuté sur une plate-forme Solaris et vous avez besoin d'une intégration CA EEM ; déplacez le module d'authentification vers un serveur d'applications, car CA SDM ne prend pas en charge l'intégration de CA EEM sous Solaris.

Remarque : CA SDM doit être installé sur le serveur externe sélectionné. Si vous déplacez le module d'authentification vers un serveur externe, il deviendra un point de défaillance unique. Par exemple, si vous déplacez le module d'authentification vers un serveur d'applications, les utilisateurs ne pourront plus pour se connecter si ce serveur d'applications tombe en panne.

Le schéma suivant illustre le déplacement du module d'authentification :


Administrateur système
Vérifier la configuration requise
Configurer CA SDM pour l'utilisation de l'authentification externe
Redémarrer les serveurs CA SDM
Vérifier l'authentification

Pour déplacer le module d'authentification vers un serveur externe, effectuez les tâches suivantes :

1. Vérifiez la configuration requise.
2. Configurez CA SDM pour le déplacement du module d'authentification. (page 353)
3. Redémarrez les serveurs CA SDM. (page 354)
4. Vérifiez l'authentification. (page 357)

Vérifiez la configuration requise.

L'analyse des plates-formes de serveur CA SDM permet de décider comment déplacer le module d'authentification vers un serveur externe.

- Identifiez le système d'exploitation du serveur suivant, en fonction du type de configuration :
  - Conventionnelle : serveur principal
  - Disponibilité avancée : serveur d'applications
- Identifiez le type d'authentification requise à partir des modèles suivants :
  - Authentification Windows pour la mise en oeuvre de CA SDM sous UNIX ou Linux
  - Authentification CA EEM pour la mise en oeuvre CA SDM sous Solaris
- Assurez-vous que CA SDM est installé sur le serveur externe sélectionné.

Configuration de CA SDM pour l'utilisation de l'authentification externe

Pour rediriger les demandes d'authentification vers un serveur externe, vous devez spécifier le nom d'hôte du serveur cible sur lequel est installé le module d'authentification. Le processus de configuration de CA SDM pour le déplacement du module d'authentification est différent pour la configuration conventionnelle et la configuration de disponibilité avancée de CA SDM.

Configuration conventionnelle

1. Connectez-vous au serveur principal en tant qu'administrateur.
2. Dans l'invite de commande, remplacez le répertoire par samples\pdmconf sous NX_ROOT et exécutez pdm_perlpdm_edit.pl.
3. Dans le menu supérieur de pdm_edit.pl, sélectionnez U, puis appuyez sur Entrée.

   Le sous-menu Serveur de validation d'utilisateur s'affiche.
4. Entrez E pour spécifier le nom d'hôte du serveur externe, puis appuyez sur Entrée.
5. Entrez Principal pour le serveur principal ou le nom d'hôte du serveur secondaire, puis appuyez sur Entrée.

Vous avez configuré la redirection des demandes d'authentification vers un serveur externe.

Configuration de disponibilité avancée

1. Connectez-vous à l'interface utilisateur Web du serveur d'arrière-plan en tant qu'administrateur.
2. Sélectionnez l'onglet Administration.
3. Développez Gestionnaire d'options, puis Sécurité.
4. Cliquez sur l'entrée bopauth_nxd_host dans la Liste des options.

   La page Détails des options bopauth_nxd_host s'ouvre.
5. Cliquez sur Modifier.
6. Dans la liste déroulante Valeur de l'option, sélectionnez le nom d'hôte du serveur cible.
7. Cliquez sur Enregistrer.

Remarque : Par défaut, le module d'authentification est exécuté sur le serveur d'arrière-plan.

Vous avez configuré la redirection des demandes d'authentification vers un serveur externe.

Procédure de redémarrage des serveurs CA SDM

Selon votre configuration de CA SDM :

- Redémarrez les serveurs CA SDM dans le cadre d'une configuration conventionnelle (page 354).
- Redémarrez les serveurs CA SDM dans le cadre d'une configuration de disponibilité avancée (page 354).

Redémarrage des serveurs CA SDM dans le cadre d'une configuration conventionnelle

Dans le cadre d'une configuration conventionnelle, redémarrez les serveurs dans l'ordre suivant :

Remarque : Pour redémarrer un serveur, cliquez sur Démarrer, Paramètres, Panneau de configuration, Outils d'administration, Services. Cliquez avec le bouton droit de la souris sur Serveur CA SDM et sélectionnez Démarrer.

1. Redémarrez le serveur secondaire.
2. Redémarrez le serveur principal.

Redémarrage des serveurs CA SDM dans le cadre d'une configuration de disponibilité avancée

Dans le cadre d'une configuration de disponibilité avancée, redémarrez les serveurs CA SDM dans l'ordre suivant :

Remarque : Pour redémarrer un serveur, cliquez sur Démarrer, Paramètres, Panneau de configuration, Outils d'administration, Services. Cliquez avec le bouton droit de la souris sur Serveur CA SDM et sélectionnez Démarrer.

1. Redémarrez tous les serveurs de secours.
2. Promouvez le serveur de secours comme nouveau serveur d'arrière-plan (page 355).
3. Démarrez l'ancien serveur d'arrière-plan.

   Lorsque vous démarrez le serveur d'arrière-plan, il est converti en serveur de secours.
4. Identifiez le serveur d'applications le moins actif (page 356).
5. Redémarrez-le.
6. Arrêtez l'autre serveur d'applications (page 356).
7. Lancez le serveur d'applications.
8. Répétez les étapes 6 et 7 pour les autres serveurs d'applications.

Promotion du serveur de secours comme nouveau serveur d'arrière-plan

Avant d'arrêter le serveur d'arrière-plan, promouvez le serveur de secours que vous avez mis à niveau comme nouveau serveur d'arrière-plan. Si l'Automatisation du soutien est installée avec CA SDM, notifiez les utilisateurs de l'Automatisation du soutien actifs de l'arrêt du serveur d'arrière-plan.

1. Exécutez la commande suivante sur le serveur d'arrière-plan pour notifier tous les utilisateurs actifs utilisant l'Automatisation du soutien afin qu'ils puissent enregistrer leur travail :

   ```
   sa_server_notifier [-h] | [-q seconds] | [-c]
   ```

   -h

   Affiche la page d'aide.

   -q seconds

   Cette option indique la mise au repos d'un serveur local (d'arrière-plan) selon l'intervalle spécifié. Cet intervalle correspond au nombre de secondes avant que le serveur ne soit mis hors ligne. Vous ne pouvez pas utiliser cette option pour un serveur de secours ou un serveur d'applications.

   -c

   Cette option annule une demande de mise au repos envoyée au préalable.

   Un message contextuel est affiché pour tous les utilisateurs actifs utilisant l'Automatisation du soutien. Ce message notifie les utilisateurs de l'arrêt du serveur et du temps restant avant l'arrêt. Les utilisateurs doivent enregistrer leur travail et se déconnecter dans l'intervalle planifié.

2. Exécutez la commande suivante sur le serveur de secours que vous souhaitez promouvoir comme nouveau serveur d'arrière-plan :

   ```
   pdm_server_control –b
   ```

   -b

   Indique à un serveur de secours local de devenir serveur d'arrière-plan. Le serveur de secours doit déjà être en cours d'exécution. Sinon, il démarrera, mais le basculement ne sera pas effectué. Pour lancer un basculement, réexécutez la commande.

   Le serveur d'arrière-plan s'arrête automatiquement et le serveur de secours est promu en tant que nouveau serveur d'arrière-plan. Ce changement n'affecte pas les sessions des utilisateurs finals. Les mises à jour en cours, le cas échéant, sont stockées et retardées, jusqu'à ce que le nouveau serveur d'arrière-plan soit mis en ligne.

Identification du serveur d'applications le moins actif

Vous choisissez le serveur d'applications sur lequel l'activité des utilisateurs est la moins importante. Exécutez la commande suivante sur chaque serveur d'applications pour choisir celui qui compte le moins de sessions actives.

```
pdm_webstat
```

Remarque : Cette commande ne capture pas les sessions de service Web SOAP ou REST.

Arrêt de l'autre serveur d'applications

Avant d'arrêter un serveur d'applications, vous informez tous les utilisateurs connectés qu'ils doivent se connecter au serveur d'applications le moins actif. Vérifiez que vous avez redémarré le serveur d'applications le moins actif avant d'y déplacer tous les utilisateurs.

1. (Recommandé) Informez tous les analystes d'Automatisation du soutien actifs sur le serveur d'applications que vous voulez arrêter, de créer un billet dans CA SDM avec leur information de session. Ce processus permet d'éviter la perte de cette information. Par exemple, l'analyste d'Automatisation du soutien est connecté à une session avec un client afin de résoudre un problème matériel. Dans ce cas, l'analyste d'Automatisation du soutien peut créer une demande client dans CA SDM avec l'information de session avant la fermeture du serveur d'applications.
2. Envoyez une notification (par exemple, une notification par courriel) à tous les utilisateurs actifs sur le serveur d'applications leur indiquant d'utiliser le serveur d'applications le moins actif que vous venez de redémarrer. Cette notification peut inclure les détails du serveur d'applications mis à jour.
3. Exécutez la commande suivante sur le serveur d'applications :

   ```
   pdm_server_control [-h] -q intervalle -s nom_serveur
   ```

   -h

   Affiche la page d'aide.

   -q intervalle -s nom_serveur

   Indique la mise au repos d'un serveur d'applications local ou distant selon l'intervalle spécifié. Cet intervalle correspond au nombre de secondes avant la mise hors ligne du serveur. Si cette option est utilisée sans la valeur nom_serveur, cela indique au serveur local de se mettre au repos. Vous ne pouvez pas utiliser cette option pour un serveur d'arrière-plan ou de secours.

Un message contextuel s'affiche pour tous les utilisateurs actifs sur le serveur d'applications, afin de les notifier de l'arrêt du serveur et du temps restant avant l'arrêt. Les utilisateurs doivent enregistrer leur travail et se déconnecter dans l'intervalle. Le serveur d'applications s'arrête après la durée spécifiée. Les utilisateurs se connectent à l'autre serveur d'applications pour reprendre leur travail. L'analyste d'Automatisation du soutien peut consulter le billet et reprendre son travail.

Le serveur d'applications est arrêté.

Vérification de l'authentification

Vérifiez l'authentification avec un ID d'utilisateur disposant d'un enregistrement de contact correspondant dans Windows ou CA EEM, en fonction du type d'authentification. Si vous pouvez vous connecter, cela signifie que le module d'authentification a été correctement déplacé.

1. Lancez le navigateur et entrez l'URL de CA SDM.
2. Connectez-vous à CA SDM avec un nom d'utilisateur disposant d'un enregistrement de contact correspondant dans Windows ou CA EEM, en fonction du type d'authentification.

Si le module a été correctement déplacé, la page d'accueil du centre de services s'ouvre.

Personnalisation de méthode de notification

Les méthodes de notification automatiques d’CA SDM permettent de notifier le personnel à des moments clés du processus de gestion du centre de service. Les méthodes de notification standard de CA SDM sont les suivantes :

- Courriel
- Notification (journal)
- Adresse_courriel_téléavertisseur

Vous pouvez définir des méthodes de notification personnalisées pour spécifier une nouvelle méthode de transmission, telle que la messagerie vocale, des panneaux d'affichage ou une imprimante spécifique. Vous pouvez également accéder aux données d’une autre application et les inclure dans le message de notification.

Processus de notification

Les notifications de tickets (applicables aux demandes client, aux demandees de changement et aux demandes) sont traitées lors de l'enregistrement du ticket, comme décrit ci-dessous.

- Si vous utilisez une autre méthode de notification, comme le courriel, le processeur de notification exécute la méthode de notification pour chaque contact de la liste. Cette méthode est généralement un script interpréteur ou exécutable qui est lancé dans un nouveau processus. Les détails concernant la notification sont stockés dans des variables d'environnement de sorte que l'exécutable ou le script puisse facilement y accéder.
- Pour chaque notification demandée, le processeur de notification définit les variables d'environnement NX_NTF_MESSAGE et NX_NTF_SUMMARY en utilisant les informations indiquées dans le titre et le corps du message de la notification dans la page de carnet Modèle du message de la fenêtre Détail des notifications d'activité. Si le destinataire correspond à un contact valide, d'autres variables d'environnement sont créées grâce aux informations de son enregistrement Détail du contact.
- Si l'option Ecrire dans le fichier est activée pour la notification, un fichier texte est créé à l'aide d'informations supplémentaires que la méthode de notification peut utiliser pour obtenir des informations plus détaillées.
- Une liste des contacts destinataires de la notification est créée à partir des informations des pages de carnet Objets, Contacts, Types et Enquête de la fenêtre Détail des notifications d'activité. Si la méthode de notification définie correspond au niveau de notification et si l'option log_all_notify du gestionnaire d'options est installée, une notification est d'abord générée dans le journal des notifications.

Variables de méthode de notification

Deux ensembles de variables sont créés et mis à la disposition de la méthode de notification.

Variables d'environnement de base

Le premier ensemble de variables est créé pour chaque notification envoyée, que vous ayez ou non sélectionné l'option Ecrire dans le fichier pour la notification. Elles sont écrites dans l'environnement comme variables d'environnement accessibles par la méthode de notification en mode standard. Si vous choisissez l'option Ecrire dans le fichier comme méthode de notification, ces variables sont également copiées dans le fichier de notification qui se trouve dans la section de notification.

Les variables d'environnement suivantes vous fournissent des informations de base sur la notification. Elles sont toujours définies, même si la valeur correspondante est vide :

Variable d'environnement	description
NX_NTF_MESSAGE	Texte du modèle de message terminé, comprenant toutes les variables complètes
NX_NTF_SUMMARY	En-tête du modèle de message terminé, comprenant toutes les variables complètes
NX_NTF_URGENCY	Urgence de la notification (1 pour basse, 4 pour urgente).

Les variables d'environnement suivantes sont créées uniquement si le destinataire est un contact CA SDM valide, auquel cas elles sont définies à l'aide des valeurs de l'enregistrement Détail du contact du destinataire, comme indiqué dans le tableau suivant :

Variable	Champs de la fenêtre Détail du contact
NX_NTF_BEEPER_PHONE	Numéro du téléavertisseur
NX_NTF_COMBO_NAME	Nom, Prénom, Deuxième prénom
NX_NTF_CONTACT	Informations de contact de ID
NX_NTF_EMAIL_ADDRESS	Courriel ou Adresse de courriel du téléavertisseur (en fonction du type de notification)
NX_NTF_FAX_PHONE	Numéro de télécopieur
NX_NTF_PUBLIC_PHONE	Numéro de téléphone
NX_NTF_USERID	ID d'utilisateur
NX_NTF_VOICE_PHONE	Autre numéro de téléphone

Remarque : Ces variables ne sont pas créées si les valeurs correspondantes sont vides (à l'exception de NX_NTF_CONTACT, qui ne peut pas être vide).

Variables d'attributs

Le deuxième ensemble de variables, appelées variables d'attribut, est disponible uniquement si vous sélectionnez l'option Ecrire dans le fichier lorsque vous définissez la méthode de notification. Ces variables sont copiées uniquement dans le fichier de notification, pas dans l'environnement. Elles se présentent sous la forme suivante :

NX_NTF_attribute[**.**secondary_attribute]=value

où :

attribut

Nom de l'attribut dont vous souhaitez obtenir la valeur. Il s'agit du nom de l'attribut tel qu'il a été défini pour l'objet. Pour une liste complète de tous les noms d'attribut pour tous les objets, reportez-vous au Manuel de référence technique de CA SDM. Les objets le plus couramment associés aux notifications sont le ticket, dont le nom d'objet est fonction du type (par exemple, cr pour les demandes), et le contact identifiant le destinataire, dont le nom d'objet est cnt. Par exemple, la variable d'environnement de l'attribut description d'un ticket peut ressembler à l'exemple suivant dans le fichier de notification :

NX_NTF_DESCRIPTION=Voici un exemple de description.

secondary_attribute

Si le premier *attribut* est l'identificateur interne d'un autre objet, un attribut secondaire est souvent ajouté, avec insertion d'un point, pour fournir des informations plus significatives. Dans une base de données, un attribut n'est pas une valeur de donnée simple, mais une clé étrangère qui pointe vers une ligne d'une autre table. L'utilisation de cette valeur de clé brute serait probablement peu utile dans ce cas. Dans un souci d'économie de temps, nombre de champs de ce type sont résolus ou déréférencés pour vous. secondary_attribute constitue alors la valeur dans la table référencée. Par exemple, au lieu d'écrire la valeur de l'attribut de la personne assignée, qui est en réalité stockée comme ID unique de l'enregistrement de contact pour la personne assignée, le nom combiné de celle-ci est écrit en se référant à l'attribut combo_name pour l'objet contact, comme indiqué dans l'exemple suivant :

NX_NTF_ASSIGNEE.COMBO_NAME=Aramis, Brigitte

Si un attribut n'a pas de valeur, la valeur correspondante est généralement (NULL) ou vide. Par exemple :

NX_NTF_CALL_BACK_DATE=(NULL)

NX_NTF_GROUP.COMBO_NAME=

Remarque : Une variable d'attribut qui existe pour le ticket et pour le destinataire est NX_NTF_ID (attribut ID), qui correspond à l'ID de base de données unique pour l'objet.

Fichier de notification

Si vous activez l'option Ecrire dans le fichier lorsque vous définissez une méthode de notification, toutes les variables d'environnement de base et les variables d'attributs sont copiées dans un fichier texte, qui est fermé avant l'exécution du script ou du programme de la méthode de notification. Ce fichier de notification est copié à chaque invocation de la méthode de notification pour un contact. Il s'agit d'un mécanisme commode pour transmettre des informations pertinentes au script de notification, qui sans cela ne sont pas disponibles dans l'environnement.

Le chemin complet du fichier de notification est défini dans la variable d'environnement NX_NTF_FILENAME, qui est à la disposition du processus de la méthode de notification. Le nom de fichier est également ajouté à la fin de la valeur que vous entrez dans le champ Méthode de notification lorsque vous définissez la méthode de notification. Par exemple, si la méthode de notification est "pdm_perl –w mymethod.pl", le processus réel exécute "pdm_perl –w mymethod.pl *nom_fichier_notification_unique*".

Important : L'administrateur peut nettoyer les fichiers de notification. Cette opération de nettoyage est particulièrement importante pour un site utilisant un volume important de notifications, car il peut y en avoir des milliers par jour. Les fichiers se trouvent dans le répertoire temporaire standard (TEMP sous Windows et TMP sous UNIX). Il est suggéré est de supprimer le fichier à la fin du script/programme de la méthode de notification.

Le fichier de notification est un fichier texte standard divisé en sections. Chaque ligne contient une paire attribut/valeur ou un marqueur de section. Chaque fichier de notification comprend trois sections, comme décrit ci-dessous. Toutes les sections commencent par les caractères « ----- » suivis d'une nouvelle ligne.

SECTION=obj, où obj identifie le type d'objet du ticket.

Iss

Fournit des informations sur la demande client.

Chg

Fournit des informations sur la demande de changement.

Cr

Fournit des informations sur la demande.

SECTION=cnt

Fournit des informations sur le destinataire.

SECTION=notification

Fournit les mêmes informations que celles figurant dans les variables d'environnement de base.

Remarque : Les noms de section du ticket et du destinataire sont en réalité les noms d'objet des attributs de la section. Pour une liste complète de tous les noms d'attribut pour tous les objets, reportez-vous au *Manuel de référence technique de CA SDM*.

Chaque section contient plusieurs lignes de paires attribut/valeur, représentant chacune un attribut de l'objet correspondant. La partie Variables d'attributs de cette section fournit des informations détaillées sur la manière dont ces lignes sont mises en forme et sur leur signification.

Les sauts de ligne dans une valeur d'attribut sont reproduits comme de nouvelles lignes dans le fichier de notification. Le processus de votre méthode de notification peut uniquement utiliser les lignes d'attribut ou de valeur qui commencent par NX_NTF et les marqueurs de section. Générez un fichier échantillon et examinez son contenu avant d'utiliser un fichier de notification dans le processus de votre méthode de notification.

Utilisation de scripts Perl

La plupart des méthodes de notification utilisent un fichier exécutable ou un script interpréteur pour lire les variables d'environnement et envoyer le message. Ceci fonctionne bien sur la plupart des serveurs UNIX, mais la lecture des variables d'environnement sur un serveur Windows présente des difficultés.

Vous pouvez utiliser un script Perl pour résoudre les problèmes d'environnement sous Windows. CA SDM comprend une installation prête à l'emploi de l'interpréteur Perl, appelée pdm_perl. Tous les scripts Perl lancés avec pdm_perl comme méthode de notification sont capables d'obtenir de façon fiable les variables d'environnement. Le script Perl peut lire et mettre en forme les valeurs de variable d'environnement et poursuivre le reste de la notification, par exemple appeler un téléavertisseur ou envoyer un courriel.

Pour les serveurs Windows, utilisez l'utilitaire launchit. L'une des fonctions de cet utilitaire consiste à appeler vos scripts ou vos programmes dans un environnement interpréteur identique à l'invite de commande avec les variables d'environnement adaptées définies.

Ainsi, si vous écrivez un script Perl nommé read_env.pl pour lire plusieurs des variables d'environnement décrites ici, vous pouvez l'invoquer pour une notification en entrant ce qui suit dans le champ Méthode de notification de la fenêtre Détail de la méthode de notification :

pdm_perl *chemin_script*/read_env.pl

Cette méthode de notification démarre l'interpréteur Perl et exécute les instructions du script read_env.pl.

Création d'une méthode de notification personnalisée

Pour créer une étape de notification personnalisée, effectuez les opérations suivantes :

1. Créez un script pour traiter le modèle de message et le transmettre au destinataire. Le script peut correspondre à tout type d'exécutable, en fonction de la plate-forme. Vous pouvez également utiliser des interpréteurs tiers ou appartenant au domaine public. Généralement, UNIX utilise des scripts d'interpréteur Bourne, et Windows des fichiers .bat. Si votre script requiert un modèle spécial, vous devez le créer.
2. Ajoutez la nouvelle méthode de notification à votre site à l'aide de l'interface Web.

Informations complémentaires :

Créer un script (page 363)
Ajouter la méthode de notification (page 364)

Créer un script

Procédez comme suit pour créer le script d'une méthode de notification :

1. Définissez la manière dont la notification doit être envoyée (par exemple, sortie sur une imprimante particulière).
2. Définissez le contenu du message de notification.
3. Spécifiez les informations du modèle de message à inclure dans la notification.
4. Définissez un script pour transmettre la notification.
5. Placez le script dans un fichier exécutable dans le chemin d'accès du serveur CA SDM.

Ajouter la méthode de notification

Lorsque vous avez créé le script, vous devez définir la nouvelle méthode de notification pour CA SDM. Il existe deux façons d'ajouter une méthode de notification :

- A l'aide de l'interface Web
- A l'aide d'un script interpréteur UNIX.

Informations complémentaires :

Ajout d'une méthode de notification à l'aide de l'interface Web (page 364)
Ajout d'une méthode de notification à l'aide d'un script interpréteur UNIX (page 365)

Ajout d'une méthode de notification à l'aide de l'interface Web

Utilisez l'interface Web pour ajouter une méthode de notification.

Pour ajouter une méthode de notification à l'aide de l'interface Web

1. Choisissez les méthodes de notification à partir de Notifications dans l'interface d'administration.

   La liste des méthodes de notification s'affiche.

2. Cliquez sur le bouton Créer.

   La fenêtre Créer une méthode de notification apparaît.

3. Renseignez les champs suivants :

   Symbole

   (Obligatoire) Identifie la méthode de notification.

   Ecrire dans le fichier

   Cochez cette case pour créer un fichier contenant les informations contextuelles de la méthode de notification.

   description

   Permet de décrire la méthode de notification.

   Méthode de notification

   Spécifiez le chemin complet du script exécutable de la méthode de notification. Si le script ou le programme peut être résolu en utilisant le chemin système, vous ne devez pas spécifier le chemin d'accès complet. Dans le cas d'un serveur Windows, vous pouvez recourir à l'utilitaire launchit.exe pour appeler votre script ou votre programme.

   Remarque : Pour plus d'informations sur l'utilitaire launchit, consultez l'*Aide en ligne*.

Remarque : Vu que la méthode de notification est exécutée à partir du serveur CA SDM, vous devez placer son script dans un répertoire accessible à partir du chemin sur le serveur ou spécifier le chemin d'accès complet au script. Sous UNIX, selon l'interpréteur que vous utilisez, vous pouvez effectuer cette vérification à l'aide de la commande suivante :

`which` *`chemin_du_script`*

Si vous rencontrez des problèmes avec les méthodes de notification, examinez les journaux du répertoire $NX_ROOT/log sous UNIX ou $NX_ROOT\log sous Windows.

Ajout d'une méthode de notification à l'aide d'un script interpréteur UNIX

Les étapes suivantes créent un script interpréteur de méthode de notification qui envoie le message de notification à l'imprimante du centre de services, SDPR2. Dans cet exemple, le message de notification sera constitué de l'en-tête de message et du texte de message du modèle de message.

1. Configurez le script interpréteur comme suit pour assembler le texte de la notification et le transmettre :

```
#!/bin/sh

echo "

A :       $NX_NTF_USERID

OBJET : $NX_NTF_SUMMARY

MESSAGE :

$NX_NTF_MESSAGE" |lp -dSDPR2
```

2. Nommez le fichier exécutable sd_print, puis placez-le dans un répertoire utilisé pour les scripts courants sur votre site, par exemple /usr/local/netbin.
3. Définissez le script interpréteur comme fichier exécutable à l’aide de chmod.
4. Choisissez les méthodes de notification à partir de Notifications dans l'interface d'administration.
5. Cliquez sur Nouveau dans le menu Fichier.

6. Renseignez ces champs :

   Symbole

   SDPR2

   description

   Envoyer la notification de sauvegarde à l'imprimante du service de service SDPR2

   Méthode de notification

   /usr/local/netbin/sd_print

7. Cliquez sur le bouton Enregistrer pour enregistrer le nouvel enregistrement. Cliquez ensuite sur Fermer la fenêtre pour fermer la fenêtre des détails.

Personnalisation des requêtes et messages

CA SDM met à votre disposition certaines fonctions vous permettant de restreindre le flux d'informations afin de pouvoir vous concentrer sur les appels, les demandes de changement et les demandes client s'appliquant à votre situation actuelle. L'une de ces fonctions permet de stocker des requêtes que vous pouvez utiliser pour ne voir que les informations pertinentes sur le tableau de résultats de l'interface Web ou d'administration. Une autre fonction vous permet de personnaliser les messages notifiant le personnel concerné des activités des billets.

Les requêtes stockées peuvent permettre de mettre l'accent sur les billets associés à l'utilisateur connecté et personnaliser les champs de compteur dans la zone du tableau de résultats des interfaces Web et d'administration. Vous pouvez personnaliser les messages de notification d'activité de manière à inclure les attributs de l'objet journal d'activité et les informations sur des billets spécifiques.

Renseignements supplémentaires :

Requêtes de tableau d'affichage (page 367)
Requêtes spécifiques à ITIL (page 374)
Personnalisation des messages de notification d'activité (page 375)

Requêtes de tableau d'affichage

L'une des tables de la base de données, Cr_Stored_Queries, définit les requêtes stockées. Ces requêtes stockées, qui sont similaires aux requêtes SQL, permettent de personnaliser les champs de compteur sur les noeuds du tableau de résultats dans les interfaces d'administration et Web. Les champs de compteur indiquent le nombre d'enregistrements correspondant à la requête. Par exemple, ils peuvent indiquer combien de types de demandes ont été affectés à l'utilisateur connecté.

Chaque utilisateur peut personnaliser les champs de compteur qui apparaissent sur son tableau de résultats (comme expliqué dans l'aide en ligne). Pourtant, l'administrateur de système doit d'abord définir les différents types de demandes qui peuvent être comptées dans ces champs de compteur comme requêtes stockées. Pour plus d'informations sur les requêtes du tableau de résultats, reportez-vous au *Manuel d'administration*.

Remarque : Les calculs des tableaux de résultats seront incorrects si les valeurs des requêtes de base de données sont égales à NULL. Par exemple, si votre requête du tableau d'affichage spécifie que assignee.organization = xyz et qu'un champ de personne assignée est vide (NULL) pour un enregistrement, cet enregistrement ne sera pas inclus dans le calcul du tableau d'affichage.

Requêtes stockées pour l'utilisateur connecté

Deux des champs devant être définis dans la fenêtre Détail de la requête stockée sont Clause Where et Etiquette. Ces deux champs peuvent contenir des expressions personnalisées pour l'utilisateur connecté. Les requêtes stockées font référence à des objets et des attributs plutôt qu'à des noms de tables et à des colonnes. Une requête stockée personnalisée pour l'utilisateur connecté est composée de deux parties, comme suit :

Objet (tel que cr pour un appel)

Ceci est généralement spécifié à gauche du signe égal (=). La syntaxe de cette partie de la requête stockée est la suivante :

att_name[.*att_name...*].*SREL_att_name*

Une requête stockée possède toujours un type, qui est un nom d'objet par rapport auquel la requête est exécutée et qui fournit le contexte de la requête. Dans la syntaxe précédente, le premier att_name doit être un nom d'attribut de l'objet contexte.

Utilisateur connecté (instance de l'objet cnt pour cet utilisateur)

Ceci doit être spécifié à droite du signe égal (=) si les tickets doivent être sélectionnés en fonction d'un attribut de l'utilisateur connecté. La syntaxe de cette partie de la requête stockée est la suivante :

@att_name[.*att_name*...].*SREL_att_name*

Remarque : Pour plus d'informations sur les objets et les attributs, reportez-vous au *Manuel de référence technique de CA SDM*.

Syntaxe de l'objet cr

Utilisez cette syntaxe si la référence désigne l'objet appel (cr) :

att_name[.*att_name...*].*SREL_att_name*

Cet exemple indique la localisation de la personne affectée au traitement du ticket. Dans cet exemple, le nom d'objet n'est pas défini, compte tenu que le type de la requête stockée implique l'objet cr :

```
assignee.location=@cnt.location AND active=1
```

Destinataire

Attribut de l'objet appel qui est mis en correspondance avec le champ Personne assignée dans la table correspondante. Par exemple, l'attribut assignee est défini dans l'objet cr par SREL agt, ce qui signifie qu'il se réfère au sous-objet agt. Le sous-objet par défaut agt fait partie de la définition de l'objet cnt.

emplacement

Attribut de l'objet cnt correspondant au champ c_l_id de la table Contact. L'attribut location est défini dans l'objet cnt par SREL loc, ce qui signifie qu'il fait référence à l'objet loc.

Clause WHERE

L'exemple suivant indique une valeur que vous pouvez coder dans une clause WHERE :

```
assignee.location=@cnt.location AND active=1
```

Compte tenu que le type de la requête stockée est une demande, cette requête permet de sélectionner toutes les demandes actives pour lesquelles l'emplacement du destinataire est le même que celui de l'utilisateur connecté.

Etiquette

Vous pouvez inclure les attributs de l'objet cnt dans des étiquettes comme dans les clauses WHERE. Voici un exemple d'utilisation d'un attribut de l'objet cnt dans une étiquette :

```
Appels de @cnt.location.name
```

Cette étiquette inclut le nom d'une localisation, par exemple Bordeaux, où Bordeaux remplace @cnt.location.name lorsque l'étiquette s'affiche dans une fenêtre. L'étiquette s'affiche sous la forme Appels de Bordeaux.

Mot-clé IN

Grâce au mot clé IN, une requête stockée peut faire référence à deux tables (ou plus) sans création de jointure, ce qui peut considérablement augmenter l'efficacité lors de l'exécution de la requête. Le code est le suivant :

```
SREL_nom_att IN ( valeur1 [, valeur2 [,…]] )
```

Par exemple, vous pouvez coder une requête de demande comme suit :

```
category.sym IN (\'Soft%\', \'Email\')
```

Ceci génère la clause WHERE SQL suivante :

```
category IN (SELECT persid FROM prob_ctg WHERE sym LIKE 'Soft%' OR sym = 'Email')
```

IN permet, entre autres, d'éviter les produits cartésiens. Par exemple, la requête suivante entraîne un produit cartésien et est particulièrement inefficace :

```
assignee.last_name LIKE 'MIS%' OR group.last_name LIKE 'MIS%'
```

Lorsque vous utilisez IN, la requête ne crée pas de produit cartésien ; en fait, elle ne crée pas de jointure du tout, comme dans l'exemple suivant :

```
assignee.last_name IN 'MIS%' OR group.last_name IN 'MIS%'
```

Remarque : Les parenthèses qui encadrent normalement la liste de valeurs à droite de IN peuvent être omises si la liste ne contient qu'une seule valeur. De même, vous devez éviter les jointures dans les partitions de données en convertissant une partition, comme dans l'exemple suivant :

```
assignee.last_name LIKE 'Smith'

converti en :

personne assignée = U'374683AA82ACE34AB999A042F3A0BA2E'
```

où :

U

indique que la valeur est un uuid.

'374683AA82ACE34AB999A042F3A0BA2E'

Les 32 caractères entre guillemets simples indiquent la représentation d'un UUID réel sous forme de chaîne.

Vous évitez ainsi la jointure même si la requête perd un peu en clarté. IN permet d'écrire la même partition, comme dans l'exemple suivant, présentant autant de clarté que la première version et pratiquement la même efficacité que la seconde :

```
assignee.last_name IN 'Smith'
```

CA SDM gère l'application de la clause IN à des listes QREL ou BREL. Par exemple, si vous recherchez toutes les demandes avec des actifs qui sont des parents d'un autre actif spécifique (doté de l'ID 374683AA82ACE34AB999A042F3A0BA2E), la clause WHERE appropriée est la suivante :

```
affected_resource.[parent]child_hier.child IN
(U'374683AA82ACE34AB999A042F3A0BA2E')
```

La première partie de la clause, *affected_resource*, est un SREL (clé étrangère) de l'objet cr (demande) pointant vers la table Network_Resource. La partie *child_hier* est une liste d'objets hier pointant vers les relations hiérarchiques. La dernière partie, *child*, constitue la première partie de la clause WHERE pour la requête secondaire IN. La partie *374683AA82ACE34AB999A042F3A0BA2E* représente la valeur de la clé étrangère correspondant à *child*. *[parent]* spécifie le renvoi de la requête secondaire. Etant donné que la valeur id est une représentation d'un UUID sous forme de chaîne, elle doit être indiquée comme telle et écrite sous la forme U'374683AA82ACE34AB999A042F3A0BA2E'

L'exemple suivant présente la requête SQL réelle générée, qui fournit toutes les demandes pour lesquelles l'actif est un parent d'un actif spécifique :

```
SELECT Call_Req.id FROM Call_Req WHERE Call_Req.affected_rc IN (SELECT hier_parent
FROM Asset_Assignment WHERE hier_child = U’374683AA82ACE34AB999A042F3A0BA2E’)
```

Pour exécuter des requêtes sur plusieurs parents, vous pouvez indiquer une liste séparée par des virgules dans la partie () de la requête SQL, comme indiqué dans l'exemple suivant :

```
affected_resource.[parent]child_hier.child IN
(U’374683AA82ACE34AB999A042F3A0BA2E’, U’374683AA82ACE34AB999A042F3A0BA2E’)
```

Le nom de l'attribut entre crochets ([]) est utilisé pour former la partie SELECT de la clause secondaire. La notation entre crochets n'est pas utilisée pour le groupe Requêtes stockées inclus dans Service Desk 6.0, comme indiqué dans l'exemple suivant :

```
(assignee = @cnt.id OR group.group_list.member IN (@cnt.id)) AND active = 1
```

Remarque : Si la notation entre crochets n'est pas utilisée, le sous-système SQL part du principe qu'il s'agit du nom d'attribut du premier symbole dans la partie de notation par insertion de point. Par chance, il apparaît ici que l’objet group_list contient un attribut nommé « group ». Si le nom était différent, la clause Where ne pourrait pas être analysée. La clause équivalente avec des crochets est illustrée comme suit :

```
(assignee = @cnt.id OR group.[group]group_list.member IN (@cnt.id)) AND active = 1
```

Remarque : Vous ne pouvez pas étendre la notation par insertion de point. Ainsi, l'exemple suivant n'est pas valide :

```
affected_resource.[parent]child_hier.child.name IN (‘chicago1’)
```

Requête en fonction de la priorité

Dans la base de données, la table des priorités (Priority) comporte deux colonnes : sym et enum. La valeur que voit l'utilisateur correspond aux valeurs sym. Quant à l'application, elle voit les valeurs sym en fonction des valeurs enum. Ici, les valeurs sym par défaut 1 à 5 sont l'inverse des valeurs enum.

Exemple :

Sym	Enum
1	5
2	4
3	3
4	2
5	1

Par conséquent, lors de l'écriture de la requête stockée, lorsque vous désignez une valeur de 5, vous recherchez en fait une priorité de 1, sauf si vous utilisez une valeur .sym pour spécifier l'attribuer à examiner.

Important : Ne modifiez pas les valeurs enum par défaut affectées par le produit. Si vous ajoutez des valeurs sym, poursuivez simplement à partir de la valeur enum la plus élevée.

Requêtes temporelles

Les périodes permettent de créer des requêtes stockées temporelles. Une période spécifie un laps de temps qui peut être relatif à la date actuelle. Par exemple, une période peut faire référence à aujourd'hui, à hier, à la semaine dernière ou au mois dernier. Une période a un nom, par exemple TODAY ou YESTERDAY. Pour désigner une période dans une requête stockée, utilisez l'une des deux fonctions intégrées suivantes :

StartAtTime (*nom-période*)

Fait référence au début du laps de temps décrit par la période.

EndAtTime (nom-période)

Fait référence à la fin du laps de temps décrit par la période.

Les règles de syntaxe des requêtes stockées exigent que le nom de la période soit entouré de guillemets simples, précédés chacun d'une barre oblique inverse. Par exemple, pour faire référence au début de la semaine dernière, vous devez spécifier :

```
StartAtTime(\'PAST_WEEK\')
```

Le passage du temps nécessite d'actualiser périodiquement les requêtes stockées contenant une référence à une période. Par exemple, l'intervalle décrit par "yesterday" est modifié à minuit. Pour l'actualiser, spécifiez l'heure de début, l'heure de fin et l'heure de déclenchement dans la fenêtre Détail de la période.

Heure de début

L'heure de début spécifie le début de la période en termes absolus ou relatifs. Le tableau ci-dessous décrit les champs de la section Heure de début de la fenêtre Détail de la période.

Année

Année explicite, telle que 2000, ou relative, telle que +1 (année suivante) ou –1 (année précédente)

Mois

Mois explicite de 1 (janvier) à 12 (décembre) ou relatif, tel que +1 (mois suivant) ou –1 (mois précédent)

Jour

Jour explicite de 1 à 31 ou relatif, tel que +1 (demain) ou –1 (hier)

Heure

Heure explicite de 0 à 24 ou relative, telle que +1 (heure suivante) ou –1 (heure précédente)

Minute

Minute explicite de 0 à 59 ou relative, telle que +1 ou –1

Heure de fin

L'heure de fin spécifie la fin de la période en termes absolus ou relatifs. Les champs Heure de fin de la fenêtre Détail de la période sont les mêmes que les champs Heure de début (page 373) de cette fenêtre.

Heure de déclenchement

Le champ Heure de déclenchement indique quand la clause WHERE d'une requête stockée contenant une référence à la période est recréée et la requête stockée actualisée. L'heure de déclenchement doit être relative à l'heure actuelle comme l'indique le tableau suivant :

Année

Doit être une année relative de –1 (année précédente) à +36 (36 années à partir de maintenant).

Mois

Doit être un mois relatif de –1 (mois précédent) à +11 (11 mois à partir de maintenant).

Jour

Doit être un jour relatif de –1 (hier) à +31 (31 jours à partir de maintenant).

Heure

Doit être une heure relative de –1 (heure précédente) à +23 (23 heures à partir de maintenant).

Minute

Doit être une minute relative de +9 (9 minutes à partir de maintenant) à +59 (59 minutes à partir de maintenant).

Requêtes spécifiques à ITIL

Les problèmes et les incidents sont des demandes présentant une ou deux valeurs dans l'attribut *type* : "I" pour Incidents et "P" pour Problèmes.

La requête stockée suivante répertorie tous les incidents que l'organisation de la personne assignée ou l'organisation du groupe fait correspondre à l'organisation de l'analyste connecté :

```
assignee.organization IN @cnt.organization OR group.organization IN
@cnt.organization) AND active = 1 AND type = \'I\'
```

Pour les problèmes, la requête est identique, à la différence près que type = \'P\'.

Personnalisation des messages de notification d'activité

Des messages de notification peuvent être envoyés automatiquement lorsque des activités de demande interviennent.

Remarque : Pour de plus amples renseignements sur les messages de notification et des instructions pour la définition des notifications d'activité, reportez-vous au *Manuel d'administration*.

Deux des champs à définir dans la fenêtre Détail des notifications d'activité sont Titre du message de la notification et Corps du message de la notification. Ces deux champs peuvent contenir des attributs de l'objet journal d'activité (alg pour Demandes/Incidents/Problèmes, chgalg pour Ordres de changement et issalg pour Demandes client). Ces trois objets journal d'activité sont pratiquement identiques et permettent d'identifier la demande spécifique associée à l'activité.

Mise en forme d'attributs pour les notifications d'activité

Vous pouvez utiliser les propriétés répertoriées ci-après pour éventuellement mettre en forme et remplacer certains attributs. Ceci peut être particulièrement utile lors de la mise en forme de notifications HTML dans lesquelles les données de l'attribut doivent être remplacées pour être en conformité avec les normes HTML.

Pour inclure une mise en forme, utilisez la syntaxe suivante :

```
@{property=value property=value:attribute_name}
```

Les paires de valeurs de propriétés sont séparées au moins par un espace et ne distinguent pas les majuscules et les minuscules. Le signe deux-points sépare les propriétés de mise en forme du nom de l'attribut. Si aucune propriété n'est répertoriée, aucune mise en forme et aucun remplacement ne sera effectué sur l'attribut.

Le tableau suivant présente les propriétés de mise en forme disponibles :

Propriété	description
DATE_FMT	Spécifie le format de date de l'attribut. Les valeurs valides sont : MM/DD/YYYY MM-DD-YYYY DD/MM/YYYY DD-MM-YYYY YYYY/MM/DD YYYY-MM-DD Valide uniquement pour les attributs Date. Les dates incorporées dans des chaînes ne sont pas concernées.

Propriété	description
ESC_STYLE=NONE | HTML | URL	Spécifie le type de « traitement » appliqué au texte formaté. Les valeurs valides sont : **NONE** Paramètre par défaut. Aucun traitement spécial n'est appliqué à aucun caractère du corps du contenu. **HTML** Un traitement spécial est appliqué aux caractères suivants, qui ont une signification dans le texte HTML : ■ & devient &amp ; ■ "_ devient &quot ; ■ < devient &lt ; ■ > devient %gt; **URL** Convertit tous les caractères autres que les lettres, les chiffres et « @*-_.#' en '%xx », où xx est le codage hexadécimal du caractère converti.
JUSTIFY=LEFT | CENTER | RIGHT | TRUNCATE| WRAP | LINE	Spécifie l'alignement du texte formaté. Les valeurs valides sont les suivantes : **TRUNCATE** (mise en forme par défaut) Tronque le texte à la valeur de la propriété WIDTH s'il s'agit d'un entier positif. Si ESC_STYLE=HTML, élimine la mise en forme HTML en remplaçant « < » et « > » par < et > (voir KEEPLINKS et KEEPTAGS). **LEFT|CENTER|RIGHT** Génère des caractères dont la largeur est exactement égale à WIDTH, en ajoutant ou en supprimant des espaces si nécessaire et en remplaçant les nouvelles lignes incorporées par un espace. Si ESC_STYLE=HTML, le texte généré est délimité par les balises <pre> et </pre>. L'argument WIDTH doit être spécifié sous la forme d'un entier positif. **WRAP** Identique à LEFT, à la différence près que le renvoi automatique à la ligne respecte les limites des mots (un saut de ligne n'est pas placé au sein d'un mot). **LINE** Identique à TRUNCATE, à la différence près que tous les sauts de ligne incorporés sont également remplacés par des balises si ESC_STYLE=HTML.
KEEPLINKS=YES|NO	Si KEEPLINKS=YES est spécifié, l'action de JUSTIFY=LINE ou JUSTIFY=TRUNCATE est modifiée pour conserver les balises d'ancrage HTML (Action :) tout en convertissant tous les autres caractères "<" et ">". Exclusion mutuelle avec KEEPTAGS. Valide uniquement si ESC_STYLE=HTML.

Propriété	description
KEEPNL=YES|NO	L'action normale de PDM_FMT consiste à convertir toutes les nouvelles lignes incorporées et les espaces qui suivent en un espace unique. Si KEEPNL=YES est spécifié, les nouvelles lignes incorporées sont conservées. Cet argument est ignoré pour JUSTIFY=LINE.
KEEPTAGS=YES|NO	Si KEEPTAGS=YES est spécifié, l'action de JUSTIFY=LINE ou JUSTIFY=TRUNCATE est modifiée pour conserver toutes les balises HTML. Exclusion mutuelle avec KEEPLINKS. Valide uniquement si ESC_STYLE=HTML.
PAD=YES|NO	Si PAD=NO est spécifié, PDM_FMT ne convertit pas les chaînes vides en un espace unique. Il s'agit de l'action normale lorsque WIDTH est différent de zéro, ou JUSTIFY est TRUNCATE ou WRAP.
WIDTH=*nn*	Lorsque la valeur est différente de zéro, spécifie que les caractères doivent avoir une largeur exactement égale à WIDTH pour la mise en forme du texte.

Par exemple, pour mettre en forme la description de la demande d'une notification HTML en remplaçant des caractères propres au HTML, en ajoutant des balises
 pour les sauts de lignes et en conservant tous les liens HTML en tant que liens, entrez la commande suivante :

```
@{ESC_STYLE=HTML JUSTIFY=LINE KEEPLINKS=YES:call_req_id.description}
```

Pour mettre en forme la valeur open_date d'une demande au format européen, entrez la commande suivante :

```
@{DATE_FMT=DD-MM-YYYY:call_req_id.open_date}
```

Attributs de l'objet journal d'activité

Pour inclure un attribut de l'objet journal d'activité, entrez ce qui suit dans le champ Titre du message de la notification ou Corps du message de la notification :

```
@{att_name}
```

Notez que le nom de l'objet (alg, chgalg ou issalg) est la valeur par défaut, et qu'il n'est donc pas nécessaire de le préciser. Par exemple, pour inclure le type de l'activité dans le titre du message, entrez ce qui suit dans le champ Titre du message de la notification (ainsi que le reste du texte que vous souhaitez voir figurer dans le titre) :

```
@{type}
```

Pour inclure la description de l'activité dans le corps du message, entrez ce qui suit dans le champ Corps du message de la notification (ainsi que le reste du texte que vous souhaitez voir figurer dans le corps du message) :

```
@{description}
```

Informations sur des ordre de changement spécifiques

Pour que les messages puissent fournir des informations sur l'ordre de changement spécifique ayant déclenché la notification, le champ Titre du message de la notification ou Corps du message de la notification doit contenir un attribut dans l'objet journal d'activité qui fait référence à l'objet ordre de changement. Entrez la référence dans ce format :

```
@{change_id.chg_att_name}
```

Dans cette référence, les informations suivantes s'appliquent :

@

Indique que cette expression doit être remplacée.

change_id

Attribut de l'objet journal d'activité qui le lie à une instanciation spécifique de l'objet ordre de changement (chg).

chg_att_name

Tout attribut de l'objet chg.

Par exemple, pour inclure la priorité de l'ordre de changement dans le titre du message, entrez ce qui suit dans le champ Titre du message de la notification (ainsi que le reste du texte que vous voulez voir figurer dans le titre) :

```
@{change_id.priority.sym}
```

Pour identifier la personne ayant rapporté l'odre de changement (Utilisateur final affecté) dans le corps du message, entrez ce qui suit dans le champ Corps du message de la notification (ainsi que le reste du texte que vous voulez voir figurer dans le corps du message) :

```
@{change_id.requestor.combo_name}
```

Si vous voulez rouvrir un ordre de changement spécifique par numéro et que vous voulez que le message apparaisse comme suit, utilisez la syntaxe suivante :

```
Rouvrir l'ordre de changement @{change_id.chg_ref_num}
```

Remarque : Pour que les messages puissent fournir des informations sur une demande client ayant déclenché une notification, le champ Titre du message de la notification ou Corps du message de la notification doit contenir un attribut dans l'objet journal d'activité qui fait référence à l'objet demande client, iss. En utilisant les informations relatives aux demandes et demandes de changement présentées dans cette section ainsi que les informations sur les objets et les attributs contenues dans le *Manuel de référence technique de CA SDM*, vous pouvez réaliser ces opérations.

Par exemple, pour inclure la priorité de la demande client dans le titre du message, entrez ce qui suit dans le champ Titre du message de la notification (ainsi que le reste du texte que vous voulez voir figurer dans le titre) :

```
@{issue_id.priority.sym}
```

Informations sur des demandes spécifiques

Pour que les messages puissent fournir des informations sur la demande spécifique ayant déclenché la notification, le champ Titre du message de la notification ou Corps du message de la notification doit contenir un attribut dans l'objet journal d'activité qui fait référence à l'objet demande. Entrez cette référence sous la forme suivante :

`@{call_req_id.cr_att_name}`

@

Indique que cette expression doit être remplacée.

call_req_id

Attribut de l'objet journal d'activité qui le lie à une instanciation spécifique de l'objet demande (cr).

cr_att_name

Tout attribut de l'objet cr.

Par exemple, pour inclure l'impact de la demande dans le titre du message, entrez ce qui suit dans le champ Titre du message de la notification (ainsi que le reste du texte que vous souhaitez voir figurer dans le titre) :

```
@{call_req_id.impact.sym}
```

Pour identifier le composant concerné dans le corps du message, entrez ce qui suit dans le champ Corps du message de la notification (ainsi que le reste du texte que vous souhaitez voir figurer dans le corps du message) :

```
@{call_req_id.affected_resource.name}
```

Si vous voulez rouvrir une demande spécifique par numéro et que vous voulez que le message apparaisse comme suit, utilisez syntaxe suivante :

```
Reopen Request @{call_req_id.ref_num}
```

Il existe d'autres mécanismes grâce auxquels des messages peuvent être envoyés, qui sont dans le contexte de la demande proprement dite (ou de l'ordre de changement ou de la demande client). Lorsque le contexte est la demande proprement dite, la partie "call_req_id" de la référence ne doit pas (et ne peut pas) être utilisée. Aussi, dans ces cas de figure, vous devez utiliser :

```
"@{ref_num}" plutôt que "@{call_req_id.ref_num}"
```

Personnalisation de l'interface Web

L'interface Web CA SDM (également appelée interface de navigation) fournit les fonctionnalités CA SDM par l'entremise d'Internet. Celles-ci incluent l'ouverture, la mise à jour, ou la clôture de billets, l'affichage et la publication d'annonces, ainsi que l'accès aux tables de données de soutien. Elles permettent de parcourir de façon indépendante la base de connaissances et de réduire ainsi le nombre d'appels au centre de services, et aussi d'améliorer les délais de résolution. Vous pouvez entièrement personnaliser l'interface Web et l'utiliser avec la plupart des navigateurs Web classiques.

Si vous avez installé et configuré l'interface Web, vous pouvez l'intégrer à votre interface Web existante ou la personnaliser pour l'adapter à vos besoins. Pour la personnalisation, familiarisez-vous avec le langage HTML et le navigateur Web utilisé sur votre site.

Remarque : La vue Conception de WSP fonctionne avec les contrôles CA SDM (PDM_MACROs). Lorsque vous travaillez sur des formulaires qui ne contiennent pas de contrôle CA SDM, vous pouvez uniquement utiliser l'onglet Source. Les formulaires Web Employé et Client ne contiennent aucun contrôle CA SDM ; par conséquent, ils apparaissent sous l'onglet Source et non sous l'onglet Conception. Certains formulaires d'analyste ne contiennent pas de contrôles CA SDM et apparaissent donc aussi sous l'onglet Source.

Important : CA SDM r12.9 n'utilise plus de fichier .mac personnalisé pour pdm_macro dans le répertoire NX_ROOT\site\mods\www\macro. Vous ne pouvez pas personnaliser de macros.

Important : Le soutien technique ne peut pas fournir d'assistance concernant la conception ou le débogage des personnalisations (ceci inclut également la documentation, par exemple, les systèmes d'aide en ligne). Nous fournissons des renseignements d'ordre général pour personnaliser l'interface Web de CA SDM. Lorsque vous effectuez vos personnalisations, n'oubliez pas que vous en êtes seul responsable. Le soutien technique de CA SDM peut vous aider à interpréter et à comprendre la personnalisation.

Le soutien relatif aux techniques de personnalisation consiste également à s'assurer que les techniques et outils fonctionnent de la manière décrite. Vous devez veiller à ne pas utiliser de fonctions non décrites et à ne pas exploiter les fonctions décrites au-delà des possibilités évoquées. Une telle exploitation sort du champ d'intervention de l'assistance technique et risque d'entraîner divers problèmes, voire une instabilité du système apparemment sans relation avec la personnalisation. C'est pourquoi le service de soutien peut être amené à vous demander de supprimer certaines personnalisations afin de reproduire les problèmes. Les sites doivent se préparer à cette éventualité en suivant attentivement les instructions relatives à toutes les modifications de l'arborescence des répertoires site mods et à la maintenance des journaux de modifications. Les sites qui opèrent des modifications fréquentes, complexes ou étendues doivent envisager d'aborder la personnalisation de CA SDM comme ils le feraient pour un projet d'ingénierie informatique, avec un contrôle rigoureux du code source, des tests et des versions contrôlées pour la production.

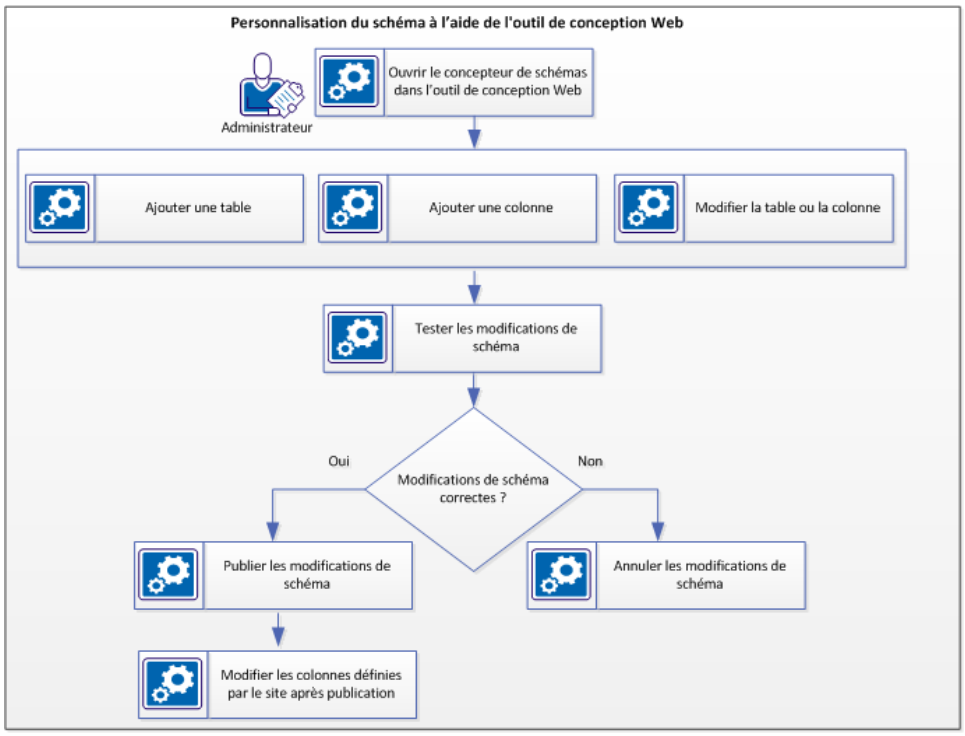
La migration des personnalisations entre versions peut présenter des défis uniques, et nous avons développé le produit de façon à préserver les efforts entrepris en termes de personnalisation. Pourtant, nous supposons toujours que le produit a été personnalisé uniquement comme indiqué dans ce manuel, particulièrement quant au placement de toutes les personnalisations dans l'arborescence mods du site. En outre, lorsque le soutien de niveau deux produit un correctif pour le système, il l'écrit en se basant sur cette même hypothèse. Corriger ou migrer un système dont les personnalisations ne sont pas rigoureuses risque souvent de se traduire par de coûteux temps d'arrêt du système. Vous pouvez l'éviter en suivant les instructions de ce manuel et en respectant quelques principes simples d'ingénierie informatique.

Remarque : Pour de plus amples renseignements sur la sécurisation et la configuration de l'interface Web, reportez-vous au *Manuel d'administration*.

Personnalisation de schémas à l'aide de l'Outil de conception Web

Pour modifier le schéma de la base de données de CA SDM, utilisez le concepteur de schémas de l'Outil de conception Web. Le concepteur de schémas propose une interface utilisateur graphique permettant de consulter et de modifier ce schéma.

Le schéma suivant illustre la personnalisation de schéma à l'aide de l'Outil de conception Web :


Personnalisation du schéma à l'aide de l'outil de conception Web
Administrateur
Ouvrir le concepteur de schémas dans l'outil de conception Web
Ajouter une table
Ajouter une colonne
Modifier la table ou la colonne
Tester les modifications de schéma
Oui
Modifications de schéma correctes ?
Non
Publier les modifications de schéma
Annuler les modifications de schéma
Modifier les colonnes définies par le site après publication

1. Consultez les remarques sur l'Outil de conception Web (page 384)
2. Ouvrez le concepteur de schémas dans l'outil de conception Web (page 384)
3. Ajoutez une table (page 385), une colonne (page 387) ou modifiez la table ou une colonne (page 393).
4. Testez les modifications apportées au schéma. Par exemple, créez, mettez à jour et affichez des formulaires Web à l'aide des schémas avant d'apporter tout changement à la base de données physique. Pour de plus amples renseignements sur la création de formulaires Web, reportez-vous à la rubrique Personnalisation de l'interface Web à l'aide de l'outil de conception Web (page 401).
   - Si elles sont correctes, publiez les modifications apportées au schéma (page 394).
   - Sinon, annulez les modifications apportées au schéma (page 399).
5. Si nécessaire, modifiez des colonnes définies par le site après la publication (page 400).

Consultation des remarques sur l'Outil de conception Web

Avant d'utiliser l'Outil de conception Web, tenez compte des renseignements suivants :

- Vous ne pouvez pas utiliser l'outil de conception Web pour modifier la longueur d'une colonne existante. Par ailleurs, il est vivement *déconseillé* d'utiliser d'autres outils pour effectuer cette opération. Les modifications apportées à la longueur d'une colonne ne sont pas prises en charge, et elles peuvent entraîner l'échec des autres applications qui accèdent à la base de données CA SDM.

  Important : Ne raccourcissez pas de champ et n'en supprimez pas, car CA SDM pourrait échouer.

- Soyez vigilant lorsque vous ajoutez des colonnes à une table, car vous pourriez dépasser involontairement la capacité de longueur d'enregistrement de la base de données dont dépend la table. Vérifiez les spécifications de la base de données que vous utilisez avec CA SDM et respectez ses limites lorsque vous effectuez des modifications.
- La publication des modifications du schéma de la base de données peut entraîner un temps d'arrêt limité ou très important, en fonction de leur nature et des capacités de votre base de données sous-jacente.
- Si vous utilisez CA SDM pour la première fois, il est plus simple d'effectuer toutes les modifications pendant les tests plutôt qu'en production.
- Vérifiez les procédures générales que vous devez effectuer avant et après avoir modifié le schéma de base de données.
- Utilisez des procédures spécifiques pour personnaliser votre schéma. La plupart de ces procédures sont suivies d'un exemple de modification que vous pouvez apporter au schéma de base de données standard.

Ouverture du concepteur de schémas dans l'outil de conception Web

Pour commencer à travailler sur le concepteur de schémas, assurez-vous que l'outil de conception Web est installé sur le serveur CA SDM. Pour de plus amples renseignements sur l'installation de l'outil de conception Web, reportez-vous au *Manuel de mise en oeuvre*.

1. Connectez-vous au serveur CA SDM suivant sur lequel l'outil de conception Web est installé, selon la configuration de CA SDM :
   - Conventionnelle : serveur principal
   - Disponibilité avancée : serveur d'arrière-plan
2. Démarrez l'outil de conception Web à l'aide d'une des actions suivantes, selon le système d'exploitation installé sur le serveur CA SDM :
   - (Windows) Dans le menu Démarrer, sélectionnez Program Files, CA, CA SDM, Outil de conception Web.
   - (UNIX) Entrez la commande pdm_wsp avec $NX_ROOT/bin dans votre chemin d'accès.

   La fenêtre de connexion de l'Outil de conception Web s'ouvre.
3. Entrez votre information d'authentification.
4. Sélectionnez Outils, Concepteur de schémas.

   La fenêtre Concepteur de schémas s'ouvre. La partie gauche de la fenêtre Concepteur de schémas affiche la base de données CA SDM sous forme d'arborescence. Les tables et les colonnes sont affichées par leur nom d'objet. Si le nom d'affichage est différent du nom d'objet de la table ou de la colonne, il apparaît entre parenthèses à la suite du nom d'objet.

Ajout d'une table

Pour ajouter une table à la base de données, utilisez le concepteur de schémas.

1. Sélectionnez Modifier, Ajouter une table.

   La boîte de dialogue Ajouter une table s'ouvre.
2. Entrez le nom de la table dans le champ Nom de la nouvelle table, puis cliquez sur OK. Veillez à ce que le nom d'une table définie par le site commence par la lettre z afin d'éviter tout conflit avec d'éventuelles futures tables standard.

   Si vous ne le faites pas, l'outil de conception Web ajoute un z au début du nom de table.

3. Remplissez les champs suivants en fonction de vos besoins :

Nom

(En lecture seule) Spécifie le nom d'objet de la table. Par exemple, le nom d'objet de la table cr est cr.

Nom d'affichage

Spécifie le nom convivial de la table. Par exemple, le nom d'affichage de la table cr est Request. Vous pouvez modifier le nom d'affichage d'une table en entrant un nouveau nom dans ce champ.

Nom du schéma

(En lecture seule pour les tables standard) Spécifie le nom utilisé pour faire référence à la table dans des utilitaires CA SDM, comme pdm_userload. Pour les tables définies par le site, le nom du schéma correspond par défaut au nom de l'objet. Vous pouvez modifier le nom du schéma en entrant une nouvelle valeur dans ce champ.

Nom du SGBD

Spécifie le nom utilisé pour faire référence à la table dans le SGBD physique. Ce champ est en lecture seule pour toutes les tables. Pour les tables définies par le site, ce nom est toujours identique au nom du schéma.

Champ d'affichage par défaut (nom commun)

Spécifie la colonne affichée dans l'interface utilisateur pour un champ qui fait référence à cette table. Par exemple, le champ Destinataire d'une demande fait référence à la table Contact. Le nom commun de la table Contact étant combo_name (nom, prénom, deuxième prénom), le nom combiné du contact référencé s'affiche à l'écran comme destinataire. Vous ne pouvez pas modifier la valeur du nom commun.

Champ de clé étrangère (attr-rel)

Spécifie la colonne stockée dans la base de données pour un champ faisant référence à cette table. Par exemple, le champ Destinataire d'une demande fait référence à la table Contact. L'attr-rel de la table Contact étant ID, la colonne Destinataire dans une demande contient l'ID du contact référencé. Vous ne pouvez pas modifier la valeur de l'attr-rel.

Groupe de fonctions

Spécifie le nom du groupe qui contrôle le niveau d'accès dont bénéficient les utilisateurs pour les enregistrements de cette table. Chaque type d'accès d'un contact détermine si celui-ci est autorisé ou non à lire ou modifier les données des tables dans chaque groupe de fonctions. Vous pouvez modifier la valeur de l'attr-rel en sélectionnant une nouvelle valeur dans la liste déroulante.

Important : Le concepteur de schémas inclut un onglet Avancé. Les données figurant dans cet onglet sont destinées au service de soutien et aux commerciaux de CA Technologies. En principe, vous n'aurez pas à employer cet onglet lors de l'utilisation du concepteur de schémas. Cet onglet ne sera pas traité plus en détail dans le présent document.

4. Pour enregistrer la table, procédez de l'une des manières suivantes :
   - Si vous travaillez sur le système de test, sélectionnez Fichier, Enregistrer.
   - Si vous travaillez sur le système de production, sélectionnez Fichier, Enregistrer et passer en mode test.

     Ainsi, vos modifications sont enregistrées dans la base de données et un fichier (wsptest.mods) est créé sur le serveur, définissant vos modifications dans le moteur d'objets. Ce fichier est stocké dans le sous-répertoire site/mods/majic du répertoire d'installation de CA SDM. Une fois le fichier wsptest.mods créé, l'outil WSP entraîne le redémarrage du moteur d'objets de façon à prendre en compte les modifications. Ce processus peut prendre de quelques secondes à quelques minutes, selon la complexité de votre schéma.

     Un message d'invite apparaît. Cliquez sur Oui pour continuer. Le fichier wsptest.mods affecte uniquement le moteur d'objets désigné par l'option wsp_domsrvr. D'autres moteurs d'objets du même serveur ne traitent pas ce fichier, et le fichier n'est pas distribué à d'autres serveurs. De plus, de nouvelles tables et colonnes en mode test sont définies dans le moteur d'objets en tant qu'objets locaux. Ceci signifie que le moteur d'objets est informé de l'existence de ces objets, et vous pouvez les utiliser dans des formulaires Web. Cependant, ces objets n'existent pas dans la base de données et n'affectent pas les autres utilisateurs. Les utilisateurs de CA SDM standard n'utilisant pas le moteur d'objets de l'outil WSP, les modifications de schéma que vous testez n'ont aucune incidence pour eux.

   La table est ajoutée.

Ajout d'une colonne

Pour ajouter une colonne à la base de données, utilisez le concepteur de schémas.

1. Sélectionnez la table à laquelle vous voulez ajouter une colonne, ou sélectionnez l'une de ses colonnes existantes.
2. Sélectionnez Modifier, Ajouter une colonne.

La boîte de dialogue Ajouter une nouvelle colonne s'ouvre.

3. Entrez le nom de la colonne dans le champ Nouveau nom de colonne, puis cliquez sur OK. Veillez à ce que le nom d'une colonne commence par la lettre z afin d'éviter tout conflit avec d'éventuelles futures colonnes standard.

   L'outil WSP vérifie que vous avez ajouté un préfixe, mais ajoute un z au début du nom de la colonne si nécessaire.

4. Remplissez les champs suivants en fonction de vos besoins :

   Nom

   (Affichage uniquement) Spécifie le nom d'objet de la colonne. Par exemple, le nom d'objet de la colonne Contact alt_phone est alt_phone.

   Nom d'affichage

   Spécifie le nom convivial de la colonne. Vous pouvez modifier le nom d'affichage d'une colonne en entrant un autre nom dans ce champ. Par exemple, le nom d'affichage de la colonne Contact alt_phone est alternative phone.

   Nom du schéma

   (En lecture seule pour les tables standard) Spécifie le nom utilisé pour faire référence à la colonne dans des utilitaires CA SDM, comme pdm_userload. Pour les tables définies par le site, le nom du schéma correspond par défaut au nom de l'objet. Vous pouvez modifier le nom du schéma en indiquant une autre valeur dans ce champ.

   Nom du SGBD

   (En lecture seule pour toutes les tables) Spécifie le nom utilisé pour faire référence à la table dans le SGBD physique. Pour les tables définies par le site, le nom du SGBD est toujours identique au nom du schéma.

   Description

   Fournit une brève description de la colonne.

   Type de champ

   (En lecture seule pour toutes les colonnes standard des tables standard et les colonnes définies par le site enregistrées) Spécifie le type de données de la colonne. Vous pouvez spécifier ou modifier le type de champ des nouvelles colonnes définies par le site en sélectionnant une valeur dans la liste déroulante. La liste suivante décrit les types de champ disponibles :

   NOMBRE ENTIER

   Indique une valeur numérique.

   CHAÎNE

   Indique une chaîne de texte. Le champ Longueur de chaîne indique le nombre de caractères dans une chaîne.

DATE

Indique une date et une heure. La valeur de nombre entier stockée dans la base de données contient le nombre de secondes écoulées depuis le 1er janvier 1970 à minuit.

DURÉE

Indique une durée. La valeur stockée dans la base de données est un entier contenant un nombre de secondes.

DOUBLE

Indique un nombre réel (virgule flottante).

SREL

Indique une référence de clé étrangère vers une autre table. Le champ Table SREL spécifie la table référencée. La valeur stockée dans la base de données est la valeur attr-rel de la table référencée ; il peut s'agir d'un entier ou d'une chaîne. La valeur qui s'affiche à l'écran correspond au nom commun de la ligne de la table référencée. Pour de plus amples renseignements sur le paramétrage d'attributs SREL avec des valeurs de clé étrangère, reportez-vous au *Manuel de référence technique*.

BREL

Indique une colonne virtuelle représentant l'ensemble des objets dotés d'une SREL pour cette table. Ce type de champ se trouve uniquement dans le moteur d'objet et n'est pas physiquement stocké dans la base de données. Avant de sélectionner ce type de champ, contactez un employé de CA Technologies.

QREL

Indique une colonne virtuelle représentant un ensemble d'objets sélectionné par la clause Where sous l'onglet Avancé. Ce type de champ se trouve uniquement dans le moteur d'objet et n'est pas physiquement stocké dans la base de données. Avant de sélectionner ce type de champ, contactez un employé de CA Technologies.

DÉRIVÉE

Indique une colonne virtuelle construite par le moteur d'objet à partir des valeurs d'autres colonnes, selon une formule spécifiée sous l'onglet Avancé. Ce type de champ se trouve uniquement dans le moteur d'objet et n'est pas physiquement stocké dans la base de données. Avant de sélectionner ce type de champ, contactez un employé de CA Technologies.

Longueur de chaîne

Longueur d'une colonne de type chaîne. Ce champ reste vide pour les autres types de colonnes. Il est par ailleurs en lecture seule pour toutes les colonnes standard ainsi que pour les colonnes définies par le site et qui ont été enregistrées. Vous pouvez indiquer ou modifier la longueur d'une nouvelle colonne de type CHAÎNE définie par le site. Il suffit pour cela d'entrer un entier compris entre 1 et 32767 dans ce champ.

Table SRel

Table référencée par une colonne de type SREL. Ce champ reste vide pour les autres types de colonnes. Il est par ailleurs en lecture seule pour toutes les colonnes standard ainsi que pour les colonnes définies par le site et qui ont été enregistrées. Vous pouvez spécifier la table référencée par une nouvelle colonne SREL définie par le site en la sélectionnant dans la liste déroulante.

Valeur par défaut lors de la création d'une nouvelle entrée

Valeur par défaut attribuée à cette colonne lorsqu'une nouvelle ligne est définie pour la table. Cette valeur doit être adaptée au type de champ. Des mots clés sont disponibles pour certains types de champs spécifiques :

MAINTENANT

Spécifie la date et l'heure actuelles d'une colonne DATE.

UTILISATEUR

Indique l'utilisateur actif pour une colonne de type SREL dans la table Contact.

Valeur définie lors de l'enregistrement

Valeur attribuée à cette colonne lorsqu'une ligne de la table est mise à jour. Cette valeur doit être adaptée au type de champ. Des mots clés sont disponibles pour certains types de champs spécifiques :

MAINTENANT

Spécifie la date et l'heure actuelles d'une colonne DATE.

UTILISATEUR

Indique l'utilisateur actif pour une colonne de type SREL dans la table Contact.

Obligatoire

Lorsque cette option est cochée, une valeur doit être proposée pour la colonne afin que vous puissiez enregistrer une ligne de la table contenant cette valeur. Vous pouvez définir cette option pour les colonnes standard et les colonnes définies par le site, et vous pouvez désactiver une option que vous avez définie. Toutefois, vous ne pouvez pas désactiver cette option pour une colonne standard à moins qu'elle n'ait été configurée par votre site.

Mise à jour possible uniquement pour les nouveaux enregistrements

Lorsque cette option est cochée, une valeur peut être proposée pour cette colonne uniquement lorsqu'une ligne de sa table est créée initialement, et la valeur ne peut donc pas être modifiée. Vous pouvez définir cette option pour les colonnes standard et les colonnes définies par le site, et vous pouvez désactiver une option que vous avez définie. Toutefois, vous ne pouvez pas désactiver cette option pour une colonne standard à moins qu'elle n'ait été configurée par votre site.

Clé pour pdm_userload

Lorsque cette option est activée, elle indique que cette colonne est l'une des colonnes testées par pdm_userload pour déterminer si la valeur entrée est une mise à jour d'une ligne existante. Cette option s'applique uniquement aux colonnes de type CHAÎNE. Elle est en lecture seule pour toutes les colonnes des tables standard.

Options de l'index du SGBD

Ces options définissent les caractéristiques d'une colonne représentant un index du SGBD physique. Elles s'appliquent uniquement aux colonnes des tables définies par le site.

Unique

Spécifie que la colonne est unique dans la table et que chaque ligne doit avoir une valeur distincte pour la colonne.

Ordre croissant

Spécifie que l'index du SGBD est présenté dans l'ordre croissant par cette colonne. Cette option et l'option Ordre décroissant s'excluent mutuellement.

Ordre décroissant

Spécifie que l'index du SGBD est présenté dans l'ordre décroissant par cette colonne. Cette option et l'option Ordre croissant s'excluent mutuellement.

Important : Le concepteur de schémas inclut un onglet Avancé. Les données figurant dans cet onglet sont destinées au service de soutien et aux commerciaux de CA Technologies. En principe, vous n'aurez pas à employer cet onglet lors de l'utilisation du concepteur de schémas. Cet onglet ne sera pas traité plus en détail dans le présent document.

5. Pour enregistrer la colonne, procédez de l'une des manières suivantes :

   - Si vous travaillez sur le système de test, sélectionnez Fichier, Enregistrer.
   - Si vous travaillez sur le système de production, sélectionnez Fichier, Enregistrer et passer en mode test.

     Ainsi, vos modifications sont enregistrées dans la base de données et un fichier (wsptest.mods) est créé sur le serveur, définissant vos modifications dans le moteur d'objets. Ce fichier est stocké dans le sous-répertoire site/mods/majic du répertoire d'installation de CA SDM. Une fois le fichier wsptest.mods créé, l'outil WSP entraîne le redémarrage du moteur d'objets de façon à prendre en compte les modifications. Ce processus peut prendre de quelques secondes à quelques minutes, selon la complexité de votre schéma.

     Un message d'invite apparaît. Cliquez sur Oui pour continuer. Le fichier wsptest.mods affecte uniquement le moteur d'objets désigné par l'option wsp_domsrvr. D'autres moteurs d'objets du même serveur ne traitent pas ce fichier, et le fichier n'est pas distribué à d'autres serveurs. De plus, de nouvelles tables et colonnes en mode test sont définies dans le moteur d'objets en tant qu'objets locaux. Ceci signifie que le moteur d'objets est informé de l'existence de ces objets, et vous pouvez les utiliser dans des formulaires Web. Cependant, ces objets n'existent pas dans la base de données et n'affectent pas les autres utilisateurs. Les utilisateurs de CA SDM standard n'utilisant pas le moteur d'objets de l'outil WSP, les modifications de schéma que vous testez n'ont aucune incidence pour eux.

   La colonne est ajoutée à la table.

Modification d'une table ou d'une colonne

Pour modifier les données concernant une table ou une colonne, dans le concepteur de schémas, cliquez dans une table ou une colonne pour la sélectionner, puis entrez les nouvelles données dans les champs appropriés. Les données susceptibles d'être modifiées dépendent de l'état de la table ou de la colonne :

Tables standard

Permet de modifier les champs Nom d'affichage, Description et Groupe de fonctions.

Colonnes standard

Permet de modifier les champs Nom d'affichage et Description, la valeur par défaut lors de la création d'une nouvelle entrée et la valeur définie lors de l'enregistrement. De plus, si les cases correspondant à Obligatoire ou Mise à jour possible uniquement pour les nouveaux enregistrements ne sont pas cochées, vous pouvez les sélectionner. Vous ne pouvez pas supprimer ces options si elles sont définies par défaut. Cependant, vous pouvez annuler vos modifications.

Table définie par le site

Si la table n'est pas publiée, vous pouvez modifier tous les champs, à l'exception du champ Nom, lequel ne peut pas être modifié après l'enregistrement de la nouvelle table. Une fois qu'une table définie par le site a été publiée, vous pouvez modifier uniquement les champs Nom d'affichage, Description et Groupe de fonctions.

Colonne définie par le site

Si la colonne est publiée, vous pouvez modifier tous les champs, à l'exception du champ Nom, lequel ne peut pas être modifié après l'enregistrement de la nouvelle colonne. Une fois qu'une colonne définie par le site a été publiée, vous pouvez modifier uniquement les champs Nom d'affichage et Description, les options Valeur par défaut lors de la création d'une nouvelle entrée et Valeur définie lors de l'enregistrement, les cases à cocher Obligatoire et Mise à jour possible uniquement pour les nouveaux enregistrements, ainsi que les options de l'index du SGBD et la clé pour pdm_userload.

Publier les modifications de schéma

Une fois que vous êtes satisfait de vos modifications de schéma, vous pouvez les publier et les mettre ainsi à la disposition de tous les utilisateurs. L'outil de conception Web stocke vos tables et colonnes, nouvelles ou mises à jour, respectivement dans les tables wsptbl et wspcol de la base de données.

1. Créez ou mettez à jour les fichiers décrivant le schéma modifié dans le moteur d'objets et les utilitaires CA SDM. L'outil WSP crée les fichiers suivants dans le moteur Web désigné par l'option wsp_webengine (avec web:local comme valeur par défaut) :

   wsp.mods

   Décrit toutes les modifications de schéma gérées par l'Outil de conception Web dans le moteur d'objets.

   wsp_schema.sch

   Décrit toutes les tables et les colonnes gérées par l'Outil de conception Web.

   wsp_index.sch

   Décrit les index du SGBD pour les tables gérées par l'Outil de conception Web.

   wsp.altercol

   Nomme les colonnes créées par l'outil WSP, mais qui n'ont pas encore été définies dans le SGBD.

   wsp.altertbl

   Nomme les tables créées par l'outil WSP, mais qui n'ont pas encore été définies dans le SGBD. De plus, l'outil WSP distribue le fichier wsp.mods à tous les serveurs CA SDM disposant d'un moteur d'objets.

2. Sélectionnez Fichier, Enregistrer et publier.

   Cette opération crée les fichiers nécessaires sur les serveurs CA SDM, mais ne démarre aucun d'entre eux. L'impact des nouveaux fichiers n'est donc pas immédiat. Cependant, une fois les fichiers créés, ils seront utilisés lors du redémarrage suivant des services CA SDM.

3. Si vous utilisez la *configuration conventionnelle*, procédez comme suit :

   - Arrêtez les services CA SDM sur le serveur principal et exécutez la commande suivante :

     ```
     pdm_publish
     ```

     Cette commande modifie le SGBD physique de sorte qu'il contienne les renseignements relatifs au nouveau schéma.

     Important : L'exécution du processus pdm_publish affecte considérablement le travail d'autres utilisateurs. Veillez à planifier avec soin la publication des changements apportés au schéma. Nous vous conseillons d'utiliser la commande Demandes de changement de CA SDM pour planifier la publication du schéma et en obtenir l'approbation.

4. Si vous utilisez la *configuration de disponibilité avancée*, procédez comme suit :

   a. Exécutez la commande suivante sur le serveur d'arrière-plan pour indiquer à tous les utilisateurs actifs utilisant l'automatisation du soutien d'enregistrer leur travail :

      ```
      sa_server_notifier [-h] | [-q seconds] | [-c]
      ```

      -h

      Affiche la page d'aide.

      -q seconds

      Cette option indique la mise au repos d'un serveur local (d'arrière-plan) selon l'intervalle spécifié. Cet intervalle correspond au nombre de secondes avant que le serveur ne soit mis hors ligne. Vous ne pouvez pas utiliser cette option pour un serveur de secours ou un serveur d'applications.

      -c

      Cette option annule une demande de mise au repos envoyée au préalable.

Un message contextuel s'affiche pour tous les utilisateurs actifs utilisant l'automatisation du soutien sur le serveur d'arrière-plan. Ce message informe les utilisateurs de l'arrêt du serveur et le temps prévu restant. Les utilisateurs doivent enregistrer leur travail et se déconnecter dans l'intervalle planifié.

b. Arrêtez les services CA SDM sur le serveur d'arrière-plan.

Important : Ne redémarrez pas les services CA SDM sur les serveurs de secours ou d'applications après l'exécution de l'option Enregistrer et Publier à partir de l'outil de conception Web. Cette action endommage la configuration de disponibilité avancée. Si les services CA SDM sur les serveurs de secours ou d'applications sont arrêtés et que vous voulez les démarrer, exécutez la commande pdm_server_control –v sur les serveurs pour supprimer le contrôle de version, puis démarrez les services CA SDM.

Important : Si le serveur d'arrière-plan échoue pendant l'opération de publication, veillez à récupérer les changements de l'outil de conception Web. Pour de plus amples renseignements, consultez la rubrique Récupération des changements de l'outil de conception Web lors d'une panne du serveur d'arrière-plan (page 398).

c. Exécutez la commande suivante sur le serveur de secours que vous souhaitez promouvoir comme nouveau serveur d'arrière-plan :

```
pdm_server_control –b
```

-b

Indique à un serveur de secours local de devenir serveur d'arrière-plan. Le serveur de secours doit déjà être en cours d'exécution. Sinon, il démarrera, mais le basculement ne sera pas effectué. Pour lancer un basculement, réexécutez la commande.

Le serveur d'arrière-plan s'arrête automatiquement et le serveur de secours est promu en tant que nouveau serveur d'arrière-plan. Ce changement n'affecte pas les sessions des utilisateurs finals. Les mises à jour en cours, le cas échéant, sont stockées et retardées, jusqu'à ce que le nouveau serveur d'arrière-plan soit mis en ligne.

d. Exécutez la commande suivante sur le serveur d'arrière-plan d'origine (désormais, le serveur de secours) pour mettre à jour le SGBD avec les changements apportés au schéma :

```
pdm_publish
```

La commande pdm_publish crée un fichier de contrôle qui entraîne la suppression de la synchronisation du serveur de secours avec le serveur d'arrière-plan lors du prochain démarrage de CA SDM. Cette action est nécessaire pour préserver les changements apportés au fichier de schéma par pdm_publish. Cette commande effectue également le deuxième basculement après la publication des modifications apportées au schéma. Le message suivant apparaît pour l'utilisateur à l'issue de la publication :

```
Voulez-vous que pdm_publish lance CA Service Desk Manager sur ce serveur de secours et effectue un basculement (O/N) ?.
```

- Si vous entrez O, pdm_publish lance les services CA SDM sur le serveur de secours et effectue automatiquement le basculement. Passez à l'étape g pour appliquer les changements apportés au schéma à tous les serveurs d'applications.
- Si vous entrez N, passez à l'étape e.

e. Démarrez les services CA SDM sur le serveur de secours (serveur d'arrière-plan d'origine).

Le démarrage détecte le fichier de contrôle créé par pdm_publish, mais ne synchronise pas le serveur de secours avec le serveur d'arrière-plan. Ainsi, les changements apportés par pdm_publish pour ce démarrage sont préservés.

Important : Veillez à suivre ces instructions de manière précise, car l'échec du basculement vers le serveur d'arrière-plan d'origine après l'exécution de pdm_publish entraîne l'endommagement des services.

f. Exécutez la commande suivante sur le serveur de secours (serveur d'arrière-plan d'origine) pour lui rendre son rôle de serveur d'arrière-plan :

```
pdm_server_control –b
```

Cette commande supprime également le fichier de contrôle, de sorte que le contrôle de version fonctionne normalement lorsque ce serveur redevient un serveur de secours.

g. Exécutez la commande suivante sur les serveurs d'applications :

```
pdm_server_control -q intervalle -s nom_serveur
```

-q intervalle -s nom_serveur

Indique la mise au repos d'un serveur d'applications local ou distant selon l'intervalle spécifié. Cet intervalle correspond au nombre de secondes avant la mise hors ligne du serveur. Si cette option est utilisée sans la valeur nom_serveur, cela indique au serveur local de se mettre au repos. Vous ne pouvez pas utiliser cette option pour un serveur d'arrière-plan ou de secours.

Un message contextuel apparaît pour tous les utilisateurs actifs sur le serveur d'applications spécifié. Ce message informe les utilisateurs de l'arrêt du serveur et le temps prévu restant. Les utilisateurs doivent enregistrer leur travail et se déconnecter dans l'intervalle planifié. Les utilisateurs se connectent au serveur d'applications mis à jour pour reprendre leur travail.

h. Redémarrez tous les serveurs de secours.

Récupération des changements de l'outil de conception Web lors d'une panne du serveur d'arrière-plan

Vous pouvez récupérer les changements du schéma de la MDB en cas d'échec du serveur d'arrière-plan lors de l'activité de publication.

Important : Nous vous recommandons de ne pas effectuer les étapes de récupération directement dans l'environnement de production. Assurez-vous de les valider d'abord dans l'environnement de test ou de développement.

- Si le serveur d'arrière-plan est tombé en panne avant la publication, les derniers changements apportés au schéma enregistrés sont conservés dans la MDB. Connectez-vous au nouveau serveur d'arrière-plan et reprenez vos tâches de publication.
- Si le serveur d'arrière-plan est tombé en panne après la publication, effectuez les opérations suivantes :

  a. Arrêtez les services CA SDM sur le serveur d'arrière-plan tombé en panne.

  b. Choisissez un serveur de secours que vous voulez désigner comme nouveau serveur d'arrière-plan.

  c. Copiez les fichiers suivants du serveur d'arrière-plan tombé en panne vers le même emplacement sur le serveur de secours :

  - "NX_ROOT/site/mods/majic/wsp.mods"
  - "NX_ROOT/site/mods/wsp.altertbl"
  - "NX_ROOT/site/mods/wsp.altercol"
  - "NX_ROOT/site/mods/wsp_index.sch"
  - "NX_ROOT/site/mods/wsp_schema.sch

d. Pour publier les changements du schéma et effectuer le basculement automatique, exécutez la commande suivante sur le serveur de secours :

```
pdm_publish
```

e. Dans le message d'invite qui s'affiche après la publication des changements apportés au schéma, sélectionnez O.

Les services CA SDM démarrent sur le serveur de secours.

Remarque : Si le basculement automatique n'intervient pas, exécutez la commande pdm_server_control -b à partir du serveur de secours pour le désigner comme nouveau serveur d'arrière-plan.

f. Mettez au repos et redémarrez chaque serveur d'applications. Redémarrez tous les serveurs de secours. Pour de plus amples renseignements, consultez la rubrique Publication des modifications de schéma (page 424).

Annuler les modifications de schéma

Si vous changez d'avis concernant vos modifications de schéma après les avoir basculées en mode test, vous pouvez rétablir la version publiée du schéma. L'annulation des modifications de schéma peut affecter d'autres utilisateurs. C'est pourquoi cette option est disponible uniquement si votre installation comprend les deux options wsp_domsrvr et wsp_webengine permettant de dédier un moteur d'objets et un moteur Web à l'outil de conception Web.

1. Sélectionnez Fichier, Revenir au mode Test.

L'outil de conception Web supprime le fichier wsptest.mods, ce qui entraîne le rétablissement de la version publiée du schéma par le moteur d'objets de l'outil de conception Web.

Après la suppression du fichier wsptest.mods, l'outil WSP entraîne le redémarrage de son moteur d'objets pour qu'il puisse recréer son schéma interne. Ce processus peut prendre de quelques secondes à quelques minutes, selon la complexité de votre schéma.

À l'issue du redémarrage du moteur d'objet, la version publiée du schéma activé est restaurée.

Remarque : Pour fonctionner avec le nouveau schéma, les formulaires Web modifiés ne sont pas automatiquement rétablis ; ils peuvent ne pas fonctionner correctement lors de leur utilisation avec le schéma publié.

Modification des colonnes définies par le site après la publication

Après la publication des modifications du schéma définies par le site, l'outil de conception Web les traite de la même manière que le schéma standard et interdit toute modification ultérieure. Vous pouvez supprimer une colonne définie par le site ou modifier la longueur d'une colonne de chaîne définie par le site en mettant manuellement à jour le SGBD et le schéma externe dans l'outil de conception Web. Puis, exécutez le script pdm_wspupd pour mettre à jour la table wspcol de la base de données de sorte à synchroniser l'outil WSP avec les modifications externes.

1. Connectez-vous au serveur ci-dessous, en fonction de votre configuration de CA SDM :
   - Conventionnelle : serveur principal
   - Disponibilité avancée : serveur d'arrière-plan
2. Recherchez le sous-répertoire site/mods dans le répertoire d'installation de CA SDM.
3. Modifiez le fichier wsp_schema.sch pour supprimer des colonnes définies inutiles par le site ou pour modifier la longueur des colonnes de chaîne définies par le site. Il s'agit des seules modifications gérées par cette procédure. Vous pouvez utiliser un éditeur de texte standard pour modifier le fichier wsp_schema.sch.

   Important : Si des options d'index (par exemple : UNIQUE) ont été spécifiées pour supprimer une colonne, modifiez le fichier wsp_index.sch et supprimez des références à la colonne. Si la colonne était la seule colonne indexée de la table, supprimez toutes les références à la table à partir du fichier wsp_index.sch.
4. Modifiez le fichier majic/wsp.mods en appliquant les mêmes changements apportés à wsp_schema.sch :
   - Supprimez les colonnes définies par le site devenues inutiles.
   - Modifiez la longueur de colonnes de chaîne définies par le site.
5. Dans l'invite de commande, entrez la commande suivante :

   ```
   pdm_wspupd
   ```

Le script pdm_wspupd lit le fichier wsp_schema.sch et le compare à la table wspcol dans la base de données en écrivant une ligne dans la console qui signale les différences. Par exemple, vous pouvez obtenir le résultat suivant :

```
PDM_WSPUPD : mettre à jour la table wspcol à partir de wsp_schema.sch

Lecture de wsp_schema.sch en cours pour obtenir les données du SGBD...

Lecture de la table wspcol en cours pour obtenir les données de schéma de WSP...

La longueur de la colonne de type chaîne zSalesOrg.description est passée de 350
à 400.

La colonne zSalesOrg.sym est introuvable dans wsp_schema.sch : suppression de la
ligne wspcol.

Le script pdm_wspupd a trouvé une colonne gérée par WSP devant être mise à jour
et 1 colonne devant être supprimée. Vérifiez que votre SGBD a été mis à jour
manuellement afin de correspondre à wsp_schema.sch, puis répondez O pour mettre
à jour wspcol, ou sinon annulez.
```

6. Vérifiez que les modifications trouvées par pdm_wspupd correspondent exactement aux modifications que vous avez effectuées dans wsp_schema.sch. Si tel est le cas, entrez **Y** pour confirmer les modifications.

   Une fois que vous avez confirmé la mise à jour, le script utilise des utilitaires standard d'CA SDM pour mettre à jour la table wspcol. Puis, le concepteur de schémas affiche vos modifications.

7. Arrêtez les serveurs CA SDM.
8. À l'aide de l'utilitaire adapté à votre SGBD, modifiez la définition de SGBD des colonnes que vous avez modifiées :

   - Supprimez toute colonne de la base de données que vous avez supprimée dans wsp_schema.sch.
   - Modifiez la longueur de base de données de toutes les colonnes de chaîne que vous avez modifiées dans wsp_schema.sch.

   Veillez à ce que les modifications apportées au SGBD correspondent exactement à celles que vous avez effectuées dans le fichier wsp_schema.sch.

9. Supprimez le fichier wsp_schema.log.
10. Publiez les modifications de schéma (page 394).
11. Démarrez les serveurs CA SDM.

Personnalisation de l'interface Web à l'aide de l'Outil de conception Web

L'outil de conception Web permet d'adapter des formulaires Web aux conditions requises de votre site sans programmation.

Toutefois, certains formulaires Gestion des connaissances ne peuvent pas être personnalisés en mode Conception de l'outil de conception Web. Pour ces formulaires, il existe d'autres approches de la personnalisation, comme suit :

- Affichage du document : le modèle de document utilisé lors de la création du document détermine le contenu de cette page. Il est possible de modifier ces modèles sous l'onglet Administration, sous Documents, Modèles de documents.
- Liste de documents de catégories de connaissances : vous pouvez modifier cette page à l'aide de l'Outil de conception Web, mais elle est également gérée par les préférences de l'utilisateur. La fenêtre Préférences permet à chaque utilisateur de personnaliser la définition des propriétés de document à afficher dans la liste de documents et le nombre de documents à afficher par page.

1. Démarrez l'Outil de conception Web (page 403).
2. Vérifiez la configuration requise (page 403).
3. Choisissez le formulaire à personnaliser (page 403) :
   - Créez un formulaire (page 404).
   - Ouvrez un formulaire existant (page 406).
4. Personnalisez un formulaire. (page 407)

   L'outil de conception Web enregistre toujours les changements sur le serveur sur lequel il est installé. Lorsque vous enregistrez un fichier, les autres utilisateurs de l'outil de conception Web peuvent y accéder dans une session d'aperçu, mais le fichier est invisible pour les utilisateurs standard de CA SDM. En effet, l'outil de conception Web enregistre tous les fichiers dans le répertoire site/mods/wsp et ce dernier n'est pas utilisé par une session CA SDM standard.
5. Si vous apportez des changements de formulaire Web dans le système de test, effectuez une migration du système de test vers le système de production (page 424).
6. Publiez des changements de formulaire (page 424).
7. (Si nécessaire) Supprimez des formulaires après la publication (page 426).

Vérifiez la configuration requise.

Avant d'initialiser la personnalisation, vérifiez les configurations suivantes :

- Personnalisez le schéma à ajouter aux formulaires Web.
- (Configuration de disponibilité avancée uniquement) Vérifiez les configurations suivantes pour la publication des formulaires Web :
  - (Recommandé) Les services CA SDM doivent être en cours d'exécution sur tous les serveurs CA SDM. Sans quoi, l'outil de conception Web effectuera la publication uniquement sur les serveurs CA SDM démarrés et en cours d'exécution.
  - (Requis) Au moins une instance de webengine doit être exécutée sur tous les serveurs CA SDM.

Démarrage de l'Outil de conception Web

Démarrez l'outil de conception Web pour personnaliser des formulaires Web.

1. Connectez-vous à l'ordinateur sur lequel l'Outil de conception Web est installé.
2. Démarrez WSP.
   - (Windows) Cliquez sur Démarrer, Programmes, CA, Service Desk, Outil de conception Web.
   - (UNIX) Entrez la commande *pdm_wsp* avec $NX_ROOT/bin dans votre chemin d'accès.

     Important : Si vous utilisez UNIX, Firefox doit être installé pour utiliser l'outil de conception Web.

   La fenêtre de connexion de l'Outil de conception Web s'ouvre.
3. Entrez votre information d'authentification.

   L'outil WSP affiche le formulaire principal.

Choix du formulaire à personnaliser

Vous pouvez créer un formulaire ou ouvrir un formulaire existant à personnaliser. Choisissez parmi les possibilités suivantes :

- Créez un formulaire (page 404).
- Ouvrez un formulaire existant (page 406).

Création d'un formulaire

Créez un formulaire dans l'outil de conception Web.

1. Cliquez sur Fichier, Nouveau.

   La boîte de dialogue Nouveau formulaire s'ouvre.

2. Remplissez les champs suivants en fonction de vos besoins :

   Interface ou type de fichier

   Indique le type de fichier du formulaire. Par exemple, pour créer un formulaire HTMPL, sélectionnez une interface (Analyste, Client, Employé, Valeur par défaut ou Assistant personnel). Pour créer un formulaire de type de fichier différent, sélectionnez le type directement (feuille de style CSS, HTML, ou JavaScript). Lorsque vous sélectionnez une interface ou un type de fichier, l'outil de conception Web affiche une liste de tous les modèles disponibles pour le type de fichier sélectionné dans le champ Nom du fichier.

   Groupe de formulaires

   Indique le groupe de formulaires (tel que défini pour votre installation de CA SDM) dans lequel vous voulez créer le formulaire ou fichier. Si vous n'en avez pas défini, seul le groupe de formulaires PAR DÉFAUT est disponible.

   Nom du fichier

   Indique le modèle de l'interface ou du type de fichier sélectionné. Un modèle contient les principales caractéristiques d'un nouveau formulaire ou fichier du type souhaité.

   Sélectionner une table pour la nouvelle liste ou le nouveau formulaire détaillé

   Indique les tables CA SDM pour lesquelles vous pouvez créer une liste ou un formulaire détaillé. Ce champ est renseigné en fonction de votre sélection d'interface (Analyste, Client, Employé, Valeur par défaut, ou Assistant personnel).

   Remarque : Un groupe de formulaires ne peut contenir qu'un seul formulaire détaillé ou de liste par table. Par conséquent, vous devez modifier un formulaire existant (au lieu d'en créer un) pour les tables possédant déjà un formulaire. Si vous souhaitez disposer de plusieurs versions d'un formulaire, créez un ou plusieurs groupes de formulaires qui contiendront les versions supplémentaires.

3. Cliquez sur Nouveau.

4. Le formulaire s'affiche avec vos personnalisations. Les deux onglets suivants sont affichés :

Conception

L'onglet Conception est disponible pour les formulaires détaillés, de liste et de barre de menus. Il présente les contrôles du formulaire disposés plus ou moins comme ils sont présentés à l'utilisateur. Le formulaire n'a pas cet aspect pour l'utilisateur final. Pour voir à quoi il ressemble, sélectionnez Outils, Aperçu.

Source

L'onglet Source est un éditeur similaire au Bloc-notes, qui permet d'examiner le code source d'un formulaire et de le modifier. Certains formulaires peuvent être modifiés uniquement sous l'onglet Source. Pour ces formulaires, la fenêtre de modification s'ouvre sous l'onglet Source, et l'onglet Conception est désactivé.

Le formulaire est prêt à être personnalisé.

Important : Lorsque vous créez ou modifiez un formulaire détaillé ou de liste, assurez-vous d'utiliser les préfixes list_ et detail_ pour nommer le fichier HTMPL. Par exemple, utilisez list_test.htmp et detail_test.htmpl. Ce préfixe permet de prévisualiser correctement un formulaire. Lorsque vous enregistrez un modèle de détail avec un nom personnalisé, vous devez également modifier manuellement la balise <PDM_WSP>. Par exemple, <PDM_WSP mode=edit preview="test.htmpl+OP=CREATE_NEW" factory=cr>.

Renseignements supplémentaires :

Création d'un groupe de formulaires Web (page 431)

Ouvrir un formulaire existant

Ouvrez un formulaire existant dans l'outil de conception Web pour le personnaliser.

1. Sélectionnez Fichier, Ouvrir.

   La boîte de dialogue Ouverture de formulaire s'ouvre.

2. Sélectionnez l'interface (analyste, client, employé, par défaut) ou le type de fichier (Feuille de style CSS, JavaScript ou HTML) et le groupe de formulaires qui contient le formulaire à modifier.

3. Sélectionnez le formulaire de votre choix dans la liste déroulante, ou entrez son nom dans la zone de texte.

   Lorsque vous entrez un nom dans la zone de texte, l'outil WSP parcourt automatiquement la liste jusqu'au premier nom correspondant aux caractères entrés. Vous pouvez utiliser la liste déroulante Fichiers présentant l'état pour restreindre la liste des fichiers affichés :

   Site modifié avec des changements dont la publication a été annulée (+)

   Limite la liste aux fichiers modifiés à l'aide de l'outil de conception Web, mais qui n'ont pas encore été publiés. Ces fichiers sont identifiés par un signe plus (+) à la suite de leur nom.

   Site modifié (*)

   Limite la liste aux formulaires modifiés sur site, qu'ils aient été publiés ou non. Les fichiers non publiés sont identifiés par un signe plus (+) à la suite de leur nom. Les modifications de site publiées sont identifiées par un astérisque (*) après le nom de fichier.

   Tout

   Présente la liste sans aucune restriction. Les fichiers non publiés sont identifiés par un signe plus (+) à la suite de leur nom. Les modifications de site publiées sont identifiées par un astérisque (*) après le nom de fichier.

4. Cliquez sur Ouvrir.

   Le formulaire s'affiche et est prêt pour la personnalisation.

Personnalisation d'un formulaire

Après avoir ouvert le formulaire à modifier dans l'outil de conception Web, vous pouvez utiliser la barre d'outils, les commandes de menu et les raccourcis pour le personnaliser. Vous pouvez effectuer la personnalisation suivante :

- Insérer un contrôle (page 407)
- Modifier les propriétés de contrôle (page 410)
- Modifier les barres de menus (page 411)
- Modifier les feuilles de style (page 415)
- Modifier le formulaire d'aperçu contextuel (page 419)
- Modifier la liste de grilles de données dans un formulaire de liste (page 421)
- Modifier les carnets dans un formulaire détaillé (page 422)
- Modifier les fichiers HTML et JavaScripts (page 423)

Insérer un contrôle

Ajoutez un contrôle dans le formulaire. Par exemple, ajoutez une zone de texte dans le formulaire.

Les contrôles susceptibles d'être insérés dans les formulaires de liste et les formulaires détaillés sont les suivants :

Contrôle	Icône	Description
Insérer une ligne		Le contrôle sélectionné devient le dernier contrôle dans la ligne actuelle (déplace les contrôles qui suivent à la ligne suivante).
Supprimer une ligne	N/D	Supprime tous les contrôles figurant sur la ligne du contrôle actuellement sélectionné.
Zone de texte		Insère une zone de texte comportant une ou plusieurs lignes pour modifier un champ de texte ou une chaîne.
Liste déroulante		Insère une liste déroulante permettant de modifier un champ validé dans une table.
Recherche		Insère un contrôle de recherche pour modifier un champ validé dans une table. Le contrôle est constitué d'une zone de texte avec un lien hypertexte dans l'étiquette qui fait apparaître un formulaire de sélection.
Bouton		Insère un bouton.

Contrôle	Icône	Description
Recherche hiérarchique		Similaire à un contrôle de recherche, à la différence près qu'il est utilisé pour un champ avec un sélecteur hiérarchique (par exemple, une catégorie d'appel).
Date		Insère un champ de date. Le contrôle est constitué d'une zone de texte avec un lien hypertexte dans l'étiquette qui fait apparaître un sélecteur de date.

Les contrôles supplémentaires suivants sont disponibles pour les formulaires détaillés uniquement :

Contrôle	Icône	Description
Case à cocher		Insère une case à cocher.
Éditeur HTML		Insère un éditeur HTML pour un champ de texte qui contient du code HTML.
Zone de texte en lecture seule		Insère un champ de texte non modifiable.
Recherche en lecture seule		Insère un champ de recherche non modifiable. Le champ est présenté sous forme de lien hypertexte pour afficher le formulaire détaillé qui le définit.
Lecture seule		Insère un champ de date non modifiable.
Carnet		Insère un carnet. Un formulaire détaillé ne pouvant comporter qu'un seul carnet, ce contrôle peut être inséré uniquement dans les formulaires qui ne contiennent pas encore de carnet.

Le contrôle supplémentaire suivant est disponible pour les formulaires de liste uniquement :

Contrôle	Icône	Description
Liste		Insère une liste. Un formulaire de liste ne pouvant comporter qu'une seule liste, ce contrôle peut être inséré uniquement dans les nouveaux formulaires de liste.

1. Cliquez avec le bouton droit de la souris à l'endroit où vous souhaitez placer le contrôle dans le formulaire et sélectionnez Insérer un contrôle.

   Une liste déroulante s'affiche.

2. Sélectionnez les options de la boîte de dialogue d'insertion de contrôle (page 409).

   Le contrôle est alors placé dans le formulaire.

3. Pour vérifier comment le formulaire s'affiche pour l'utilisateur final, sélectionnez Outils, Aperçu. Bien que cette fenêtre ressemble à une fenêtre CA SDM standard et que la plupart des boutons et des menus soient fonctionnels, il ne s'agit pas d'une session standard ; vous ne devez donc pas l'utiliser de cette manière.

4. Cliquez sur Fichier, puis sur Enregistrer.

   Les contrôles sont ajoutés au formulaire.

Options de la boîte de dialogue Insérer un contrôle

Dans le menu Fichier, ouvrez la boîte de dialogue Insérer un contrôle. Tous les contrôles de l'interface utilisateur correspondant à la section du formulaire sélectionné pour modification y sont répertoriés.

La boîte de dialogue contient les options suivantes :

Insérer avant

Insère le contrôle sélectionné dans la liste avant le contrôle sélectionné dans le formulaire de base, et devient le contrôle actuellement sélectionné.

Insérer après

Insère le contrôle sélectionné dans la liste après le contrôle sélectionné dans le formulaire de base, et devient le contrôle actuellement sélectionné.

Préc.

Le contrôle précédent le contrôle actuellement sélectionné devient le contrôle sélectionné dans le formulaire.

Suivant

Le contrôle suivant le contrôle actuellement sélectionné devient le contrôle sélectionné dans le formulaire.

Propriétés

Ouvre la boîte de dialogue Propriétés pour le contrôle sélectionné.

Fermer

Ferme le formulaire Insérer un contrôle.

Fermer le formulaire après insertion

(Activé) Insère le contrôle sélectionné et ferme la boîte de dialogue Insérer un contrôle lorsque vous cliquez sur Insérer avant ou Insérer après.

(Désactivé) Insère le contrôle sélectionné lorsque vous cliquez sur Insérer avant ou Insérer après. La boîte de dialogue Insérer un contrôle reste ouverte pour vous permettre d'insérer d'autres contrôles ou des propriétés de demande pour le contrôle actuellement sélectionné. Une fois que la case à cocher Fermer le formulaire après insertion est désactivée, elle le reste jusqu'à sa réactivation ou la fermeture de l'outil de conception Web.

Valeur par défaut : Activé

Modification des propriétés de contrôle

Modifiez les propriétés d'un contrôle.

1. Sélectionnez le contrôle et appuyez sur F4.

   La boîte de dialogue Propriétés s'ouvre.

2. Modifiez les propriétés selon vos besoins. Par exemple, la propriété Légende permet de spécifier l'étiquette d'en-tête qui s'affiche au-dessus d'un contrôle. Pour définir cette propriété, entrez la valeur de votre choix dans la cellule située à droite de la propriété Légende.

3. Fermez la boîte de dialogue Propriétés.

4. Pour vérifier comment le formulaire s'affiche pour l'utilisateur final, sélectionnez Outils, Aperçu. Bien que cette fenêtre ressemble à une fenêtre CA SDM standard et que la plupart des boutons et des menus soient fonctionnels, il ne s'agit pas d'une session standard ; vous ne devez donc pas l'utiliser de cette manière.

5. Cliquez sur Fichier, puis sur Enregistrer.

   Les propriétés du contrôle sont modifiées et le formulaire est enregistré.

Modification de barres de menus

Les formulaires dont le nom commence par *menubar_* définissent une barre de menus. Le mode Conception d'une barre de menus affiche le menu au-dessus. Vous pouvez cliquer sur un élément de menu pour abaisser le menu, mais vous ne pouvez pas modifier la barre de menus directement en mode Conception. Pour modifier la barre de menus, cliquez deux fois sur l'élément de menu pour afficher le concepteur de menus.

Remarque : Les menus (et les formulaires de barre de menus) sont utilisés uniquement dans l'interface analyste. Les interfaces client et employé utilisent une "barre de lancement" contenant les liens réels et non des menus déroulants. Pour personnaliser la barre de lancement client ou employé, modifiez le formulaire std_body_site.htmpl dans l'interface appropriée.

1. Sélectionnez Outils, Concepteur de menus ou double-cliquez sur le menu affiché sous l'onglet Conception d'un formulaire de barre de menus.

   La boîte de dialogue Concepteur de menus s'ouvre.

2. Pour ajouter ou modifier des éléments de menu, remplissez les champs de la boîte de dialogue Concepteur de menus (page 412). Pour de plus amples renseignements sur l'ajout d'éléments de menu, reportez-vous à la rubrique Fonctions utiles dans les éléments de menu (page 414).

3. Cliquez sur OK pour fermer la boîte de dialogue.

4. Pour vérifier comment le formulaire s'affiche pour l'utilisateur final, sélectionnez Outils, Aperçu. Bien que cette fenêtre ressemble à une fenêtre CA SDM standard et que la plupart des boutons et des menus soient fonctionnels, il ne s'agit pas d'une session standard ; vous ne devez donc pas l'utiliser de cette manière.

5. Cliquez sur Fichier, puis sur Enregistrer.

   La barre de menus est modifiée dans le formulaire.

Boîte de dialogue Concepteur de menus

Remarque : Vous pouvez accéder au concepteur de menus uniquement lors de la modification des formulaires HTMPL dont le nom commence par "menubar_", tels que menubar_admin.htmpl.

Cette boîte de dialogue apparaît lorsque vous sélectionnez Concepteur de menus dans le menu Outils ou double-cliquez sur le menu qui s'affiche sous l'onglet Conception d'un formulaire de barre de menus. Cette boîte de dialogue vous permet d'ajouter des barres de menus, des menus, des sous-menus et des commandes de menu dans le formulaire ouvert. La boîte de dialogue Editeur de menus contient les contrôles suivants :

Liste de menus

Dans cette liste, sélectionnez l'élément de menu à modifier. Par exemple, pour changer l'étiquette du menu, sélectionnez-la dans la liste, entrez un nouveau nom dans la zone de texte Légende, puis cliquez sur Appliquer.

Ajouter

Cliquez sur ce contrôle pour ajouter un élément à la fin de la liste des menus.

Insérer

Cliquez sur ce contrôle pour insérer un nouvel élément au-dessus de l'élément sélectionné dans la liste des menus.

Supprimer

Cliquez sur ce contrôle pour supprimer l'élément sélectionné de la liste des menus.

 Cliquez ici pour déplacer l'élément de menu sélectionné vers le niveau supérieur.

 Cliquez ici pour déplacer l'élément de menu sélectionné vers le niveau inférieur.

 Cliquez ici pour déplacer l'élément de menu sélectionné d'un niveau vers la droite, par exemple si vous souhaitez définir l'élément en tant que sous-menu ou commande plutôt qu'en tant que menu.

 Cliquez ici pour déplacer l'élément de menu sélectionné d'un niveau vers la gauche, par exemple si vous souhaitez définir l'élément en tant que menu plutôt qu'en tant que sous-menu ou commande.

Remarque : Le nombre de niveaux de retrait est limité à un.

Légende

Entrez le nom de l'élément de menu sélectionné. Reportez-vous à la propriété Légende pour de plus amples renseignements.

Fonction

Entrez la fonction JavaScript à exécuter lorsque l'utilisateur clique sur le menu. Pour de plus amples renseignements, reportez-vous à la description de la propriété Fonction, qui fournit notamment des fonctions prédéfinies pouvant être utiles pour la définition de menus.

ID

Entrez l'ID HTML/JavaScript à attribuer à l'élément de menu.

Touche d'accès rapide

Entrez une liste de caractères indiquant à CA SDM votre préférence quant à la touche d'accès rapide de cet élément de menu. La lettre correspondant à la touche d'accès rapide apparaît soulignée dans la légende du menu lorsque l'affichage est activé. CA SDM sélectionne généralement la première lettre de la légende du menu qui n'est pas déjà utilisée comme touche d'accès rapide. Vous pouvez cependant indiquer dans ce champ un ou plusieurs caractères afin de limiter la sélection à ces caractères, ou les faire précéder d'un point d'exclamation en vue d'empêcher leur sélection.

Image

Indiquez l'emplacement de l'image que vous souhaitez voir apparaître en regard de l'élément de menu.

Interne

Sélectionnez cette option pour indiquer que le code JavaScript appelé par la fonction doit être exécuté dans le contexte de la fenêtre en cours (qui peut être une fenêtre de détail contextuelle). Si cette option est désélectionnée, la fonction est exécutée dans le contexte du formulaire principal.

Variable

Entrez la variable JavaScript à attribuer à l'élément de menu.

Barre d'outils

Ajoute une icône de barre d'outils et une info-bulle correspondant à un élément de menu de niveau non supérieur.

Fichier d'icône

Identifie l'emplacement de l'icône de barre d'outils.

TIP

Spécifie le texte de l'info-bulle.

OK

Cliquez sur ce contrôle pour fermer la boîte de dialogue et enregistrer vos modifications.

Annuler

Cliquez sur ce contrôle pour fermer la boîte de dialogue sans enregistrer les modifications.

Fonctions utiles dans les éléments de menus

CA SDM affiche, dans la plupart des formulaires, une barre de menus qui permet de contrôler ses fonctions. La barre de menus est générée par un formulaire HTMPL avec un nom du formulaire menubar_*xx*.htmpl. Nous vous recommandons d'utiliser l'outil WSP pour personnaliser les barres de menus existantes et en définir de nouvelles.

Les fonctions prédéfinies suivantes peuvent être utiles pour les scripts appelés par des éléments de menus :

upd_frame(form)

Permet de charger un nouveau formulaire dans le cadre de contenu de la fenêtre principale.

create_new(factory, use_template, width, height [,args])

Fait apparaître un formulaire permettant de définir un nouvel enregistrement.

Popup_window(name, form[, width, height [,features [,args]]])

Fait apparaître une nouvelle fenêtre.

showDetailWithPersid(persid)

Fait apparaître un enregistrement de détail.

Les termes et les définitions suivantes s'appliquent aux fonctions précédentes :

Formulaire

Il s'agit soit d'un nom de fichier HTMPL sous la forme xxx.htmpl, soit d'un code d'opération (par exemple, CREATE_NEW).

factory

Il s'agit du nom d'un objet de base de données.

use_template

La valeur est soit True (vrai), soit False (faux).

width

Ceci représente la largeur souhaitée du formulaire ou zéro par défaut.

height

Ceci représente la hauteur souhaitée du formulaire ou zéro par défaut.

features

Il s'agit d'une liste de fonctions de fenêtre, au même format que celui utilisé avec la fonction standard window.open.

args

Il s'agit d'une ou de plusieurs balises sous la forme "keyword=value" pour l'opération spécifiée pour le formulaire.

persid

Il s'agit d'un ID persistant sous la forme factory:ID.

Modification de feuilles de style

Vous pouvez utiliser l'outil WSP pour créer ou modifier des fichiers CSS (cascading stylesheet).

Remarque : Pour des raisons de performances, les feuilles de style CA SDM sont fournies sous deux formes : des fichiers individuels (tels que search_filter.css) et des fichiers combinés regroupant un certain nombre de fichiers individuels, débarrassés des commentaires et espaces superflus (tels que analyst_styles.css). L'outil de conception Web modifie systématiquement chaque fichier ; vous ne pouvez pas modifier directement un fichier combiné. Lorsque vous publiez les modifications de feuilles de style, l'outil de conception Web génère automatiquement le fichier combiné associé si nécessaire.

1. Créez ou ouvrez un fichier de feuille de style CCS.

   L'outil de conception Web affiche le mode source de la feuille de style.

2. Vous pouvez effectuer les modifications directement en mode source ou afficher le concepteur de styles en sélectionnant Outils, Concepteur de styles.

3. Remplissez les champs dans la boîte de dialogue Concepteur de styles (page 416), comme il convient. Notez que plusieurs attributs de style, tels que la marge et la bordure, ne peuvent être ni visualisés ni modifiés dans le concepteur de styles. Ils doivent être modifiés en mode Source.

4. Cliquez sur OK dans le concepteur de styles.

   L'outil de conception Web formate à nouveau la feuille de style et met à jour le mode source.

5. Cliquez sur Fichier, puis sur Enregistrer.

   La feuille de style est personnalisée.

Boîte de dialogue Concepteur de styles

La boîte de dialogue Concepteur de styles permet de modifier ou de personnaliser les feuilles de style. A l'ouverture de la boîte de dialogue, l'onglet Police et couleur est activé par défaut. Il contient les contrôles suivants :

Classes de styles

Dans la liste déroulante, sélectionnez un élément de style à modifier.

Ajouter

Cliquez sur ce contrôle pour ajouter une nouvelle classe de style.

Renommer

Cliquez sur ce contrôle pour renommer la classe de style sélectionnée dans la liste déroulante.

Supprimer

Cliquez ici pour supprimer la classe de style sélectionnée dans la liste déroulante.

Polices installées

Cette propriété répertorie les polices installées sur le système. Cliquez sur  et  pour déplacer les polices sélectionnées entre la liste Polices installées et la liste Polices sélectionnées.

Polices sélectionnées

Cette propriété définit une liste hiérarchique contenant les polices favorites qu'utilise le navigateur pour afficher l'élément de la classe de style. Les navigateurs utilisent la première police de la liste installée sur le système sur lequel ils sont eux-mêmes exécutés.

Cliquez sur  et  pour déplacer les polices sélectionnées vers le haut ou vers le bas dans la hiérarchie.

Taille de la police

Sélectionnez une taille de police dans la liste déroulante.

Gras

Sélectionnez un style de police dans la liste déroulante.

Italique

Sélectionnez un style de police dans la liste déroulante.

Sans effet

Sélectionnez cette option si vous ne souhaitez appliquer aucun effet ni ornement spécial au texte.

Souligné

Sélectionnez cette option pour souligner le texte.

Barré

Sélectionnez cette option pour barrer le texte.

Surligné

Sélectionnez cette option pour qu'une ligne apparaisse au-dessus du texte.

Couleur de premier plan

Pour sélectionner la couleur de premier plan du texte, cliquez sur le bouton Parcourir situé à droite de cette propriété, puis sélectionnez une couleur dans la palette de couleurs et cliquez sur OK.

Couleur d'arrière-plan

Pour sélectionner la couleur d'arrière-plan du texte, cliquez sur le bouton Parcourir situé à droite de cette propriété, puis sélectionnez une couleur dans la palette de couleurs et cliquez sur OK.

Transparent

Sélectionnez cette option pour que l'arrière-plan de l'élément de style soit transparent.

Un exemple de cet élément s'affiche dans la zone d'aperçu, dans la partie inférieure de la boîte de dialogue.

Pour définir la position de l'élément, cliquez sur l'onglet Position. Cet onglet comporte les contrôles suivants :

Position

Sélectionnez la position de l'élément dans la liste déroulante. Cette propriété place l'élément dans une position statique, absolue ou relative. La valeur Statique a pour effet de placer l'élément par rapport au flux normal. La valeur Absolue permet de placer l'élément n'importe où sur la page. La valeur Relative permet de déplacer l'élément par rapport à sa position normale.

Gauche

Entrez une valeur définissant la marge gauche de l'élément. Sélectionnez une taille dans la liste déroulante. Cette propriété est désactivée si vous avez choisi la position Statique.

Haut

Entrez une valeur définissant la marge supérieure de l'élément. Sélectionnez une taille dans la liste déroulante. Cette propriété est désactivée si vous avez choisi la position Statique.

Largeur

Entrez une valeur définissant la largeur de l'élément. Sélectionnez une taille dans la liste déroulante.

Hauteur

Entrez une valeur définissant la hauteur de l'élément. Sélectionnez une taille dans la liste déroulante.

Z-Index

Entrez une valeur définissant l'ordre de pile de l'élément. L'élément possédant l'ordre de pile le plus élevé est toujours placé devant un élément dont l'ordre de pile est inférieur. Z-index s'applique uniquement aux éléments ayant une position Absolue.

Remarque : Les éléments peuvent posséder des ordres de pile négatifs.

Cliquez sur l'onglet Autre pour définir des propriétés propres à l'élément. Cet onglet contient les contrôles suivants :

Visibilité

Sélectionnez le type de visibilité de l'élément dans cette liste déroulante. Cette propriété définit la façon dont le contenu d'un élément s'affiche en cas de dépassement de la zone définie.

Dépassement

Sélectionnez le type de dépassement de l'élément dans cette liste déroulante. Cette propriété détermine la solution à adopter lorsqu'un élément dépasse la zone qui lui est attribuée.

Afficher

Sélectionnez le type d'affichage de l'élément dans cette liste déroulante. Cette propriété définit le mode d'affichage de l'élément.

Curseur

Sélectionnez le type de curseur de l'élément dans cette liste déroulante. Cette propriété définit le type de curseur à afficher lorsque l'utilisateur pointe sur un élément.

OK

Cliquez sur ce contrôle pour fermer la boîte de dialogue et enregistrer vos modifications.

Annuler

Cliquez sur ce contrôle pour fermer la boîte de dialogue Concepteur de styles.

Modification d'un formulaire d'aperçu contextuel

Les aperçus contextuels permettent d'afficher des données clés dans le formulaire actuel sans devoir cliquer sur un lien ou ouvrir une page Web. L'aperçu contextuel s'affiche lorsque vous placez, pendant un certain temps, le curseur sur le lien d'un objet situé dans un formulaire détaillé ou dans un formulaire de liste. Si vous déplacez la souris avant que le délai ne s'écoule, l'aperçu ne s'affichera pas. Les aperçus contextuels s'affichent par défaut sur tous les formulaires détaillés et les formulaires de liste en lecture seule.

Vous pouvez créer des aperçus contextuels pour des formulaires ne disposant pas de paramètre preview_forms par défaut. Vous pouvez également créer des aperçus contextuels pour des formulaires personnalisés créés dans votre environnement CA SDM.

Les formulaires prenant en charge la fonctionnalité d'aperçu contextuel prédéfinis suivants sont disponibles :

- preview_chg.htmpl (Demande de changement)
- preview_cnt.htmpl (Contact)
- preview_cr.htmpl (Demande)
- preview_in.htmpl (Incident)
- preview_iss.htmpl (Demande client)
- preview_KD.htmpl (Document de connaissances)
- preview_nr.htmpl (Elément de configuration)
- preview_pr.htmpl (Problème)

1. Ouvrez l'un des formulaires suivants à personnaliser :
   - Ouvrez un formulaire existant qui ne dispose pas de paramètre preview_form par défaut. Par exemple : detail_loc.htmpl
   - Ouvrez un formulaire d'aperçu contextuel existant. Par exemple : preview_chg.htmpl.
2. Personnalisez le formulaire. Par exemple, ajoutez ou supprimez des contrôles personnalisés.
3. Cliquez sur Fichier, Enregistrer sous, puis spécifiez un nom de fichier au moyen de preview_prefix et cliquez sur Enregistrer. Par exemple, entrez preview_loc.htmpl.

   Le formulaire d'aperçu contextuel est créé et personnalisé.

Chapitre 8: Modification de liste de grilles de données dans un formulaire de liste

Les listes de grilles de données vous permettent d'afficher le contenu d'une page de produit sur un formulaire de liste sans ouvrir de page. Ce contrôle permet de répertorier les éléments de la source de données dans une table pour que vous puissiez sélectionner des éléments, les trier et extraire des données. Par exemple, les options Développer et Réduire dans le formulaire Liste des incidents.

1. Ouvrez un formulaire de liste.
2. Localisez la zone bleue située après les champs étiquetés à la fin du formulaire en mode Conception. Si vous préférez le mode Source, la grille de données s'affiche entre les lignes de code suivantes :

   ```
   <PDM_MACRO name=lsStart>
   <PDM_MACRO name=lsEnd>
   ```

   Les exemples suivants présentent la grille de données en mode Conception :

   Le signe plus dans la zone de grille de données représente le début de la section extensible de la ligne, c'est-à-dire les champs qui sont uniquement affichés lorsqu'un utilisateur clique sur plus dans la ligne de la grille du formulaire de liste. Le code suivant génère le signe plus en mode Source :

   ```
   <PDM_MACRO name=lsCol attr=open_date label="Open Date" sort="DESC" startrow=yes>
   ```

   Le paramètre *startrow=yes* indique le début d'une ligne et le début de la section extensible de la ligne.
3. Effectuez un glisser-déposer des colonnes pour les déplacer dans une liste. Vous pouvez déplacer des colonnes entre la partie principale de la ligne et la section extensible. Vous ne pouvez pas déplacer un contrôle existant après la zone de grille.
4. Pour insérer une colonne de liste, cliquez avec le bouton droit de la souris sur un contrôle ou dans l'arrière-plan bleu, puis sélectionnez Insérer une colonne ou Insérer un contrôle.
   - Si vous sélectionnez Insérer une colonne, l'outil de conception Web insère une colonne à gauche du contrôle actuellement sélectionné.
   - Si vous sélectionnez Insérer un contrôle, l'outil de conception Web affiche la boîte de dialogue Insérer un contrôle qui vous permet d'ajouter le contrôle souhaité au formulaire.

5. Pour vérifier comment le formulaire s'affiche pour l'utilisateur final, sélectionnez Outils, Aperçu. Bien que cette fenêtre ressemble à une fenêtre CA SDM standard et que la plupart des boutons et des menus soient fonctionnels, il ne s'agit pas d'une session standard ; vous ne devez donc pas l'utiliser de cette manière.
6. Cliquez sur Fichier, puis sur Enregistrer.

   La liste de grille de données est modifiée dans le formulaire de liste.

Modification de carnets dans un formulaire détaillé

Le contrôle des onglets imbriqués (carnet) vous permet de développer ou de réduire les données clés dans le formulaire actuel. Par exemple, utilisez ce contrôle pour personnaliser l'organisation des onglets dans le formulaire détaillé Incident. En mode Conception, vous pouvez utiliser le contrôle Carnet pour ajouter des onglets imbriqués à un formulaire détaillé qui n'en contient aucun. Double-cliquez sur le contrôle Carnet pour le modifier. Utilisez la fonction glisser-déposer pour ajouter, insérer, supprimer des onglets de carnet, ou modifier leurs légendes. Vous pouvez aussi utiliser les touches Haut et Bas pour réorganiser les onglets en modifiant la position de l'onglet actuellement sélectionné. La case à cocher Nouvelle ligne spécifie si l'onglet sélectionné démarre une nouvelle ligne dans l'en-tête du carnet.

1. Ouvrez un formulaire détaillé.
2. En mode Conception, localisez la zone bleue du formulaire qui contient la première étiquette numérotée.

   Si vous préférez le mode Source, la zone de carnet s'affiche entre les lignes de code suivantes :

   ```
   <PDM_MACRO name=startNotebook hdr=cng_nb>
   <PDM_MACRO name=endNotebook>
   ```

   Remarque : Dans CA SDM r12.6, un carnet peut contenir des onglets imbriqués. Dans l'outil de conception Web, un onglet de niveau supérieur (un onglet contenant d'autres onglets) est également appelé groupe d'onglets. L'outil de conception Web affiche un groupe d'onglets sous la forme d'une barre bleue pleine placée en travers de la zone de carnet bleue, avec au centre, une étiquette numérotée. Un onglet de niveau inférieur (un onglet qui ne contient pas d'autres onglets) est nommé simplement onglet. L'outil de conception Web affiche les onglets de niveau inférieur sous la forme de rectangles aux coins arrondis.

3. Cliquez sur un onglet pour le sélectionner. En sélectionnant un onglet, un lien est mis en surbrillance et affiche le contenu de l'onglet dans la partie inférieure du carnet.

   Vous pouvez déplacer les onglets et les groupes d'onglets à l'intérieur d'un carnet à l'aide de la fonction glisser-déposer. En déplaçant un groupe d'onglets, vous déplacez tous les onglets qu'il contient.

4. Pour insérer un onglet ou un groupe d'onglets, cliquez avec le bouton droit de la souris sur un contrôle ou sur l'arrière-plan du carnet bleu et sélectionnez Insérer un onglet, Insérer un groupe d'onglets ou Insérer un contrôle.

   Si vous sélectionnez Insérer un onglet ou Insérer un groupe d'onglets, l'outil de conception Web insère un onglet ou un groupe d'onglets à gauche du contrôle actuellement sélectionné. Si vous sélectionnez Insérer un contrôle, l'outil de conception Web affiche la boîte de dialogue Insérer un contrôle qui vous permet d'ajouter le contrôle souhaité au formulaire.

5. Pour vérifier comment le formulaire s'affiche pour l'utilisateur final, sélectionnez Outils, Aperçu. Bien que cette fenêtre ressemble à une fenêtre CA SDM standard et que la plupart des boutons et des menus soient fonctionnels, il ne s'agit pas d'une session standard ; vous ne devez donc pas l'utiliser de cette manière.

   Cliquez sur Fichier, puis sur Enregistrer.

Modification de fichiers HTML et JavaScript

Vous pouvez utiliser le mode Source de l'outil de conception Web pour modifier des formulaires HTML et JavaScript. Ouvrez un fichier HTML ou JavaScript et apportez les changements nécessaires.

Remarque : Pour des raisons de performances, certains fichiers JavaScript de CA SDM sont livrés sous deux formes : des fichiers individuels (tels que window_manager.js) et des fichiers combinés regroupant un certain nombre de fichiers individuels, exempts des commentaires et espaces superflus (tels que std_head.js). L'outil de conception Web modifie systématiquement chaque fichier ; vous ne pouvez pas modifier directement un fichier combiné. Lorsque vous publiez les modifications de script, l'outil de conception Web génère automatiquement le fichier combiné associé si nécessaire.

Migration du système de test vers le système de production

L'un des objectifs de l'outil de conception Web consiste à sécuriser le développement et le test des modifications de formulaire dans une base de données de production. Les fonctions telles que l'arborescence de l'Outil de conception Web sur le serveur, les processus serveur Outil de conception Web dédiés et les sessions d'aperçu en lecture seule contribuent à cet objectif. Cependant, bon nombre d'utilisateurs préfèrent élaborer leurs modifications de formulaire dans un système de test indépendant, puis migrer les formulaires dans un système de production distinct, comme ceci :

1. Copiez les formulaires HTMPL à migrer du sous-répertoire approprié site/mods/www/htmpl du système de test vers le même sous-répertoire site/mods/wsp/project du système de production.
2. Copiez tous les fichiers CSS, JavaScript et HTML à migrer du sous-répertoire approprié site/mods/www/wwwroot du système de test vers le même sous-répertoire site/mods/www/wwwroot/wsp/project du système de production.

   Remarque : Assurez-vous de copier les fichiers et les formulaires sur les serveurs suivants du système de production, selon la configuration de CA SDM :

   - Conventionnelle : serveur principal
   - Disponibilité avancée : serveur d'arrière-plan

Remarque : Vous pouvez utiliser toute méthode de copie de fichier prise en charge par votre système d'exploitation pour procéder à la copie décrite aux étapes 1 et 2 ci-dessus. Les utilisateurs Windows doivent remplacer la barre oblique (/) par une barre oblique inverse (\) dans les chemins de répertoires indiqués.

Publication de changements de formulaire

Lorsque vous êtes satisfait des modifications, vous pouvez les publier de manière à les mettre à la disposition de tous les utilisateurs de CA SDM. La publication met à jour tous les serveurs CA SDM en intégrant les nouveaux formulaires ou les formulaires modifiés.

1. Sélectionnez Fichier, Publier.

   Si des modifications n'ont pas été enregistrées, l'outil WSP vous invite à les enregistrer, puis affiche une boîte de dialogue de confirmation qui répertorie toutes les modifications de l'Outil de conception Web en attente (notamment celles enregistrées dans des sessions antérieures ou celles enregistrées par d'autres utilisateurs de Outil de conception Web). Par défaut, toutes les modifications sont sélectionnées afin d'être publiées. Vous pouvez modifier la sélection des modifications devant être publiées en cliquant dessus.

2. Lorsque la sélection vous convient, cliquez sur OK.
3. (Configuration de disponibilité avancée uniquement) Si le moteur Web n'est exécuté sur aucun serveur CA SDM, un message d'erreur s'affichera avec la liste des serveurs CA SDM sur lesquels la publication par l'outil de conception Web a échoué. Effectuez les opérations suivantes :
   a. Configurez le serveur CA SDM (serveur spécifié dans le message d'erreur) pour appliquer les corrections.
   b. Modifiez le fichier dans l'outil de conception Web et ajouter un espace dans la macro <PDM_IF 0>, puis enregistrez-le.
   c. Revenez à l'étape 1 pour republier le formulaire Web.

      Remarque : Si vous ne voulez pas apporter de changements à la configuration, vous devez copier manuellement le dossier nx_root/site/mods/www du serveur d'arrière-plan vers tous les autres serveurs.
4. (Configuration de disponibilité avancée uniquement) Si le serveur d'arrière-plan tombe en panne lors de la publication, récupérez les changements de HTMPL (page 425).
5. (Formulaires d'aperçu contextuel) Exécutez la commande suivante après la publication des changements :

   ```
   pdm_webcache -H
   ```

   Le cache Web est actualisé. L'outil de conception Web rend les changements sélectionnés disponibles pour tous les utilisateurs actifs sur tous les serveurs.

Récupération des changements HTMPL

Vous pouvez récupérer les changements HTMPL lorsque le serveur d'arrière-plan échoue lors de l'activité de publication.

Important : Nous vous recommandons de ne pas effectuer les étapes de récupération directement dans l'environnement de production. Assurez-vous de les valider d'abord dans l'environnement de test ou de développement.

1. Accédez au répertoire suivant sur le serveur d'arrière-plan en panne :

   ```
   $NX_ROOT$/site/mods/www/wwwroot/wsp/project/web
   ```
2. Copiez tout le contenu du dossier Web.
3. Connectez-vous au nouveau serveur d'arrière-plan et collez tout le contenu copié dans le dossier NX_ROOT/site/mods/www/wwwroot/wsp/project/web.
4. Reprenez la publication des changements sur le nouveau serveur d'arrière-plan. Pour de plus amples renseignements, consultez la rubrique Publication des changements de formulaire (page 424).

Suppression de formulaires après la publication

Seuls les formulaires modifiés par le site peuvent être supprimés. Les demandes de suppression d'un formulaire préalablement publié prennent effet lorsque vous publiez les modifications.

Pour annuler une demande de suppression en attente, sélectionnez Fichier, Annuler la suppression du formulaire. Vous annulez les modifications d'un formulaire après la publication ; le seul recours pour modifier un formulaire publié consiste à le modifier de nouveau.

Modèles HTML (Formulaire HTMPL)

Les formulaires de l'interface Web de CA SDM sont fournis comme modèles HTML, dans des fichiers portant le suffixe .htmpl. On les appelle formulaires HTMPL dans le reste de ce document.

Un formulaire HTMPL contient du code HTML standard (y compris JavaScript) plus des extensions de langage qui sont interprétés par un démon serveur (ou service) CA SDM appelé moteur Web, lequel transmet le code HTML standard au navigateur. Ces extensions sont répertoriées ci-après.

- Références à des variables serveur : celles-ci sont indiquées par un nom commençant par le symbole du dollar. Il peut s'agir de valeurs de colonnes de la base de données CA SDM, de références aux propriétés de configuration du moteur Web ou d'autres informations de serveur.
- Balises spéciales : celles-ci indiquent au moteur Web qu'il doit effectuer des tâches sur le serveur (par exemple, lire des informations de la base de données CA SDM). Ces balises portent des noms de type <PDM_...> ou <pdm_...>.

Remarque : Il n'est pas nécessaire de maîtriser les extensions HTMPL ni même le langage HTML proprement dit pour pouvoir personnaliser des formulaires CA SDM à l'aide de l'outil WSP.

Renseignements supplémentaires :

Variables serveur (page 453)
Balises HTMPL (page 431)

Conventions d'affectation des noms de modèles

Les conventions d'affectation de noms suivantes sont utilisées pour identifier les quatre principaux types de fichiers HTMPL (*xxx* représente l'objet).

Type de modèle	Nom
Liste (filtre de recherche et résultats)	list_*xxx*.htmpl
Formulaire détaillé combiné, en lecture seule et de modification (interface analyste)	detail_*xxx*.htmpl
Formulaire détaillé en lecture seule	detail_*xxx*_ro.htmpl
Formulaire détaillé de modification	detail_*xxx*_edit.htmpl

Vous pouvez trouver les définitions des objets et leurs propriétés aux emplacements suivants :

- (UNIX) $NX_ROOT/bopcfg/majic/*.maj
- (Windows) *répertoire-installation*\bopcfg\majic*.maj

Pour plus d'informations sur les objets et attributs qui définissent CA SDM, reportez-vous au *Manuel de référence technique de CA SDM*.

Répertoires HTMPL

Le *Manuel d'administration* décrit les interfaces Web fournies avec CA SDM. Vous disposez de plusieurs ensembles de fichiers HTMPL pour mettre en oeuvre ces interfaces, comme indiqué dans le tableau suivant :

Système d'exploitation	Répertoire des fichiers HTMPL
Windows	*répertoire-installation*\bopcfg\www\htmpl\web*interface*
UNIX	$NX_ROOT/bopcfg/www/htmpl/web/*interface*

Dans ce tableau, *interface* est le nom de l'interface (analyste, client ou employé).

Remarque : Il n'existe pas de répertoire distinct pour les fichiers de l'interface invité ; par défaut, celle-ci utilise les fichiers de l'interface employé. Si vous souhaitez modifier l'interface utilisateur invité, modifiez le type d'accès associé à l'utilisateur System_Anonymous. Les fichiers client et employé se modifient dynamiquement en fonction de l'utilisateur actuel (invité ou utilisateur connu), à l'aide de la commande du modèle <PDM_IF> décrite dans ce document.

Le répertoire htmpl contient trois sous-répertoires d'interfaces supplémentaires :

default

Contient les fichiers HTMPL communs à toutes les interfaces. Lors de la recherche d'un fichier, le moteur Web effectue d'abord une recherche dans le répertoire correspondant à l'interface de l'utilisateur actuel, puis dans le répertoire par défaut.

pda/analyst : (UNIX)

pda\analyst : (Windows)

Contient les fichiers HTMPL utilisés par l'interface périphérique mobile. Dans Unicenter Service Desk r11.0, l'interface périphérique mobile est uniquement disponible pour les analystes.

web/*interface*/legacy : (UNIX)

web*interface*\legacy : (Windows)

Contient les fichiers HTMPL de votre version précédente de CA SDM qui ne sont plus utilisés. Ce répertoire est créé automatiquement lors de l'installation de CA SDM si vous effectuez une mise à niveau à partir d'une version précédente. Vous pouvez supprimer le répertoire legacy si vos fichiers personnalisés n'utilisent aucun de ses fichiers.

Il est fortement déconseillé de modifier directement les fichiers HTMPL fournis. Utilisez plutôt l'outil WSP, ou copiez manuellement le fichier que vous voulez modifier dans le répertoire site mods, puis modifiez-le à cet emplacement. Le serveur Web CA SDM recherche un nouveau formulaire dans le répertoire site mods approprié avant de vérifier le répertoire de distribution. Les répertoires site/mods standard de chaque interface sont les suivants :

Système d'exploitation	Répertoire des fichiers HTMPL modifiés par le site
Windows	***répertoire-installation**site**mods**www**htmpl**interface**interface***
UNIX	$NX_ROOT/site/mods/www/htmpl/*interface/interface*

Remarque : Si vous modifiez le formulaire et l'enregistrez dans le répertoire *répertoire-installation**site**mods**www**htmpl**interface*, tous les utilisateurs peuvent y accéder, quel que soit le groupe de formulaires auquel ils appartiennent. Si vous l'enregistrez dans le répertoire *répertoire_installation*\site\mods\www\htmpl\interface*interface*, seuls les contacts appartenant à ce groupe de formulaires peuvent afficher les formulaires modifiés.

Dans le tableau précédent, *interface* correspond au nom de l'interface (analyste, client ou employé). Il n'existe pas de répertoire distinct pour les fichiers de l'interface Invité ; celle-ci utilise les fichiers de l'interface Employé. Il est préférable de stocker les fichiers HTMPL modifiés dans le répertoire site mods, car ce répertoire n'est pas supprimé lorsque vous installez une mise à niveau ou une nouvelle version de CA SDM. De plus, en conservant d'une part les fichiers modifiés dans le répertoire site mods, de l'autre les fichiers d'origine, vous disposez en permanence d'une copie du fichier HTMPL original distribué.

Chaque page de l'interface Web est associée à une fonction principale, comme indiqué dans le tableau ci-dessous répertoriant les principaux modèles HTML. Cependant, vous pouvez ajouter des blocs <PDM_FORM> à un modèle pour accéder directement à l'une des opérations prises en charge par l'interface Web. Par exemple, vous pouvez modifier le menu principal pour inclure des champs de soumission d'une demande client sans devoir passer par la page intermédiaire. Vous pouvez également ajouter des champs de critères de recherche et un bouton de recherche à un formulaire de liste :

Page Web	Modèle HTML
Formulaire principal	menu_frames.htmpl
Affichage/création/mise à jour d'une demande de changement	detail_chg.htmpl
Affichage de la liste des demandes de changement	list_chg.htmpl
Affichage/création/mise à jour d'une demande client	detail_iss.htmpl
Affichage de la liste des demandes client	list_iss.htmpl
Affichage/création/mise à jour d'une demande	detail_cr.htmpl
Affichage de la liste des demandes	list_cr.htmpl
Affichage des détails d'une annonce	detail_cnote_html
Affichage d'une liste d'annonces	list_cnote.html
Connexion	login.htmpl

Remarque : Pour obtenir la liste complète des modèles, consultez le contenu des répertoires dans le tableau présenté au début de cette section.

Groupes de formulaires Web

Vous pouvez rassembler des pages Web personnalisées dans un ou plusieurs groupes de formulaires. Les répertoires de groupes de formulaires sont situés dans les répertoires suivants :

Windows

répertoire-installation\site\mods\www\htmpl\web*interface*

répertoire-installation\site\mods\www\wwwroot\sous-répertoire

UNIX

$NX_ROOT/site/mods/www/htmpl/web/*interface*

$NX_ROOT/site/mods/www/wwwroot/sous-répertoire

Chaque groupe de formulaires correspond à un sous-répertoire de ces répertoires. Vous pouvez spécifier le répertoire de formulaires personnalisés dans le champ Groupe de formulaires de personnalisation du type d'accès.

Lorsqu'un utilisateur demande un formulaire, le moteur Web recherche d'abord dans le répertoire des groupes de formulaires personnalisés approprié, puis dans le répertoire standard de l'interface Web de l'utilisateur, et enfin dans le répertoire par défaut. Vous pouvez définir plusieurs types d'accès pour la même interface Web, chacun étant associé à un groupe de formulaires personnalisés différent. Ceci vous permet de définir quelques formulaires spécialisés pour différents types d'utilisateurs, tout en continuant à utiliser la majorité des formulaires de l'interface standard.

Un processus similaire intervient lorsqu'une page Web demande un fichier issu de l'un des sous-répertoires de wwwroot (css, html, img ou scripts). Le moteur Web examine une référence HTMPL du formulaire CAisd/img/xxx.gif et la convertit en l'un des fichiers GIF suivants, en sélectionnant le premier dans lequel il détecte xxx.gif :

- /CAisd/sitemods/img/formgroup/xxx.gif
- /CAisd/sitemods/img/xxx.gif
- /CAisd/img/xxx.gif

Création d'un groupe de formulaires Web

Effectuez les opérations suivantes pour créer un groupe de formulaire Web :

1. Si vous souhaitez disposer d'un groupe de formulaires en complément des groupes de formulaires Analyste, Client ou Employé prédéfinis, créez un groupe. Pour ce faire, sélectionnez Enregistrer sous dans le menu Fichier de l'outil WSP, puis cliquez sur Ajouter un groupe de formulaires dans la boîte de dialogue Enregistrer le formulaire sous. Par exemple, pour offrir deux versions personnalisées distinctes de l'interface Analyste, vous pouvez créer des groupes de formulaires nommés Analyste1 et Analyste2 pour les gérer. Vous pouvez également définir un nouveau groupe de formulaires si l'interface que vous définissez n'a pas sa place, logiquement, dans l'un des groupes de formulaires prédéfinis.
2. Dans le client Web (et non dans une session d'aperçu de l'Outil de conception Web), sélectionnez Sécurité, Types d'accès dans le menu Administration. Cliquez sur un type d'accès (ou créez-en un), puis utilisez la liste déroulante Groupe de formulaires de personnalisation dans la fenêtre Détail du type d'accès pour affecter un groupe de formulaires à un type d'accès. CA SDM détermine le type d'accès lorsqu'un contact se connecte et utilise un groupe de formulaires de personnalisation pour déterminer où rechercher les formulaires personnalisés dans la structure du répertoire site mods. Si le moteur Web ne trouve pas de formulaire dans le répertoire du groupe de formulaires, il recherche le type d'accès de l'utilisateur d'abord dans le répertoire standard, puis dans le répertoire par défaut.
3. Dans l'outil WSP, sélectionnez Enregistrer dans le menu Fichier, ou copiez manuellement les fichiers HTMPL personnalisés dans le répertoire suivant :

   Sous Windows : répertoire *répertoire-installation*\site\mods\www\htmpl\web\ *nom_groupe_formulaires*

   Sous UNIX : $NX_ROOT/site/mods/www/htmpl/web/*nom_groupe_formulaires*

Après avoir défini un nouveau groupe de formulaires Web et copié les fichiers sous-jacents nécessaires dans les sous-répertoires appropriés, vous devez redémarrer le service Web pour que les modifications soient appliquées.

Balises HTMPL

Cette section présente les commandes PDM pour ajouter des balises HTMPL.

Renseignements supplémentaires :

PDM_EVAL : Insérer la valeur d'une variable de préprocesseur (page 432)
PDM_FORM : Démarrer un formulaire HTML avec un ID de session (page 432)
PDM_FMT : Mettre en forme du texte à partir d'une variable serveur (page 433)
PDM_IF : Traitement conditionnel (page 436)
PDM_INCLUDE : Insertion à partir d'un fichier différent (page 437)
PDM_JSCRIPT : Inclure sous conditions un fichier JavaScript (page 438)
PDM_LINK : Créer un lien hypertexte appelant une opération HTMPL (page 439)
PDM_LIST : Mettre en forme une liste de lignes d'une base de données (page 439)
PDM_MACRO : Insérer du texte à partir d'un fichier de macro (page 442)
PDM_NOTEBOOK : Créer un carnet (page 449)
PDM_PRAGMA : Spécifier les informations du serveur (page 449)
PDM_SCOREBOARD : Générer une arborescence du tableau de résultats (page 450)
PDM_SET : Définir la valeur d'une variable serveur (page 451)
PDM_TAB : Créer un onglet dans un carnet (page 451)
PDM_WSP : Contrôle de l'aperçu de l'outil de conception Web (page 452)

PDM_EVAL : Insérer la valeur d'une variable de préprocesseur

La balise pdm_eval permet d'insérer la valeur d'une variable de préprocesseur dans l'entrée de l'analyseur de moteur Web. Si elle est utilisée dans une macro, son incidence est différée tant que la macro n'est pas terminée.

La balise pdm_eval fonctionne de la même manière que la balise pdm_include ou pdm_macro. Elle insère le texte dans l'analyseur à l'emplacement de la balise, exactement comme si la valeur de sa variable avait été codée à la place de la balise.

La balise pdm_eval présente la syntaxe suivante :

```
<PDM_EVAL TEXT=PRE.nom>
```

nom

(Obligatoire) Nom de la variable de préprocesseur dont la valeur est insérée dans l'entrée du moteur Web.

PDM_FORM : Démarrer un formulaire HTML avec un ID de session

Vous pouvez ajouter les balises <PDM_FORM> et </PDM_FORM> dans n'importe quel modèle HTML d'interface Web pour créer un formulaire HTML incluant deux champs masqués pour les ID de session (SID) et les ID de formulaire (FID) des variables de serveur. L'opérande OP facultatif crée un champ masqué complémentaire pour l'une des opérations gérées, comme avec la balise PDM_LINK. Sauf dans le cas des champs masqués générés automatiquement, les balises <PDM_FORM> et </PDM_FORM> sont utilisées de la même manière que les balises HTML standard <form> et </form> (et génèrent ces balises lors de leur extension).

PDM_FMT : Mettre en forme du texte à partir d'une variable serveur

Les balises <PDM_FMT> et </PDM_FMT> permettent de mettre en forme des blocs de texte insérés par des variables serveur ($args.xxx) conformément aux indications données par leurs arguments.

Remarque : La balise <PDM_FMT> est ignorée pour les littéraux, y compris les variables $prop.xxx.

Le tableau suivant décrit ces balises :

Propriété	description
ESC_STYLE=**NONE** | C | HTML | JS | JS2 | URL	Spécifie le type de « traitement » appliqué au texte formaté. Les valeurs valides sont : **NONE** Paramètre par défaut. Aucun traitement spécial n'est appliqué à aucun caractère du corps du contenu. **C** Un traitement spécial est appliqué aux caractères ', ", \, \r, ` et \n, qui ont une signification dans les programmes C. Ces caractères seront ignorés. **HTML** Un traitement spécial est appliqué aux caractères suivants, qui ont une signification dans le texte HTML : & devient & ' devient ' " devient " < devient < > devient %gt; **JS** Un traitement spécial est appliqué aux caractères suivants, qui ont une signification dans le texte JavaScript : ' devient %27 " devient %22 / devient %2F \ devient %5C \r devient %0D \n devient %0A **JS2** Identique à JS, mais aucun traitement spécial n'est appliqué au caractère /, et un traitement spécial est appliqué à deux caractères supplémentaires : - % devient %25 - Les sauts de ligne portent le suffixe %0A **URL** Convertit tous les caractères autres que les lettres, les chiffres et « @*-_.#' en '%xx », où xx est le codage hexadécimal du caractère converti.

Propriété	description
JUSTIFY=LEFT | CENTER | RIGHT | **TRUNCATE**| WRAP | LIN	Spécifie l'alignement du texte formaté. Les valeurs valides sont les suivantes : **TRUNCATE** Paramètre par défaut. Elimine la mise en forme HTML en remplaçant « < » et « > » par < et > **Remarque :** Pour plus d'informations, voir les informations ci-après sur KEEPLINKS et KEEPTAGS. **LEFT|CENTER|RIGHT** Génère des caractères dont la largeur est exactement égale à WIDTH, en ajoutant ou en supprimant des espaces si nécessaire, en remplaçant les nouvelles lignes incorporées par un espace et en délimitant le texte généré par les balises <pre> et </pre>. L'argument WIDTH doit être spécifié sous la forme d'un entier positif. **WRAP** Identique à LEFT, à la différence près que le renvoi automatique à la ligne respecte les limites des mots (un saut de ligne n'est pas placé au sein d'un mot). **LINE** Identique à TRUNCATE, à la différence près que tous les sauts de ligne incorporés sont également remplacés par des balises .
KEEPLINKS=YES|**NO**	Si KEEPLINKS=YES est spécifié, l'action de JUSTIFY=LINE ou JUSTIFY=TRUNCATE est modifiée pour conserver les balises d'ancrage HTML (Action :) tout en convertissant tous les autres caractères « < » et « > ». Exclusion mutuelle avec KEEPTAGS.
KEEPNL=YES|**NO**	L'action normale de PDM_FMT consiste à convertir toutes les nouvelles lignes incorporées et les espaces qui suivent en un espace unique. Si KEEPNL=YES est spécifié, les nouvelles lignes incorporées sont conservées. Cet argument est ignoré pour JUSTIFY=LINE.
KEEPTAGS=YES|**NO**	Si KEEPTAGS=YES est spécifié, l'action de JUSTIFY=LINE ou JUSTIFY=TRUNCATE est modifiée pour conserver toutes les balises HTML. Exclusion mutuelle avec KEEPLINKS.
PAD=**YES**|NO	Si PAD=NO est spécifié, PDM_FMT ne convertit pas les chaînes vides en un espace unique. Il s'agit de l'action normale lorsque WIDTH est différent de zéro, ou JUSTIFY est TRUNCATE ou WRAP.
WIDTH=*nn*	Lorsque la valeur est différente de zéro, spécifie que les caractères doivent avoir une largeur exactement égale à WIDTH pour la mise en forme du texte.

Si les propriétés WIDTH ou JUSTIFY ne sont pas définies, <PDM_FMT> ne met pas en forme le texte délimité mais le place entre les balises <pre> et </pre>.

Par exemple, pour générer une description sur plusieurs lignes, entrez la commande suivante :

```
<PDM_FMT WIDTH=50 JUSTIFY=WRAP>$args.description</PDM_FMT>
```

Pour générer une sortie sur plusieurs colonnes, entrez la commande suivante :

```
<PDM_FMT><PDM_FMT WIDTH=20 JUSTIFY=LEFT>$cst.last_name</PDM_FMT>
 <PDM_FMT WIDTH=20 JUSTIFY=LEFT>$cst.first_name</PDM_FMT>
  <PDM_FMT WIDTH=20 JUSTIFY=TRUNCATE>$cst.middle_name</PDM_FMT>
</PDM_FMT>
```

PDM_IF : Traitement conditionnel

Ces balises permettent d'inclure du texte sous condition. Des blocs <PDM_IF> peuvent être placés n'importe où dans un fichier HTMPL ; dans le code HTML, JavaScript et même les balises HTML. <PDM_IF> et <PDM_ELIF> (else if) n'utilisent pas des paires nom-valeur, mais une clause conditionnelle simple en tant que propriétés. Si la clause est True (vrai), le texte situé entre la balise et la balise de fermeture est inclus dans le fichier ; si la clause est False (faux), le serveur supprime le texte entre la balise et la balise de fermeture. La balise de fermeture peut être <PDM_ELIF>, <PDM_ELSE> ou </PDM_IF>.

Les balises <PDM_ELSE> et <PDM_ELIF> sont facultatives. Si vous les utilisez toutes les deux, toutes les balises <PDM_ELIF> doivent précéder <PDM_ELSE>. Il peut y avoir un nombre quelconque de balises <PDM_ELIF> entre <PDM_IF> et <PDM_ELSE> (ou </PDM_IF> si vous ne définissez pas <PDM_ELSE>).

La syntaxe de la condition dans <PDM_IF> et <PDM_ELIF> est la suivante :

- 0 est faux , tout autre nombre est vrai
- “” est False; “*any-string*” est True
- "*value op value*" compare les valeurs à droite et à gauche en fonction de l'opérateur *op* indiqué. Si ces valeurs sont uniquement numériques (éventuellement précédées d'un signe - ou +), la comparaison est effectuée numériquement. Sinon, la comparaison est lexicale (classement ASCII). Valeurs *op* valides :

Valeur op	description
==	Egal à
!=	Différent de
>=	Supérieur ou égal à (utilisez la notation \>= ou >=)
<	Inférieur à (utilisez la notation \< ou <)

Valeur op	description
>	Supérieur à (utilisez la notation \> ou >)
<=	Inférieur ou égal à (utilisez la notation \<= ou <=)
&	Effectue une opération de bits AND sur la valeur de gauche et la valeur de droite. True (Vrai) si l'un des bits est activé ; sinon False (Faux).
%	Renvoie True si la valeur de gauche est un multiple pair de la valeur de droite, sinon la valeur est False (utile pour créer des tables bidimensionnelles).
:	Procède à une comparaison de modèle orientée octet, à l'instar de la commande UNIX grep. Renvoie True (Vrai) si la valeur de gauche contient l'expression régulière définie par la valeur de droite.

Exemple :

```
<PDM_IF $count \>= 10> . . .
<PDM_ELIF $count &lt; 5>  . . .
<PDM_ELSE> . . .
</PDM_IF>
```

Une instruction PDM_IF peut contenir plusieurs conditions. Les conditions sont séparées par des connecteurs && (et) ou || (ou). Aucun connecteur ne prévaut sur l'autre. Le moteur Web examine une instruction conditionnelle de gauche à droite, jusqu'à atteindre le connecteur. Si la condition initiale est vraie et que le connecteur est ||, il considère que la condition toute entière est vraie, sans autre évaluation. Si la condition initiale est fausse et que le connecteur est &&, il considère que la condition toute entière est fausse, sans autre évaluation. Sinon, il considère la condition comme indéterminée et évalue la condition située après le connecteur.

PDM_INCLUDE : Insertion à partir d'un fichier différent

La balise <PDM_INCLUDE> permet d'insérer du texte à partir d'un second fichier dans un fichier HTMPL. Le serveur remplace la balise <PDM_INCLUDE> par le contenu du second fichier.

Les fichiers inclus peuvent contenir des balises <PDM_INCLUDE>. La profondeur de l'imbrication n'est soumise à aucune limite.

La balise <PDM_INCLUDE> gère les propriétés suivantes :

Propriété	description
FILE=nomdefichier	(Obligatoire) Spécifie le fichier à inclure. Le moteur Web recherche les fichiers HTMPL dans les répertoires utilisés, selon les définitions données dans le type d'accès de l'utilisateur actuel.

Propriété	description
FIXUP=[**YES**|NO]	(Facultatif) Indique si l'interface Web doit interpréter le fichier comme un modèle HTML normal (par exemple, en développant les variables qui commencent par le signe $ et en interprétant les autres balises CA SDM telles que PDM_LIST et PDM_FORMAT. La valeur YES indique que le fichier sera traité comme un modèle HTML normal, et la valeur NO qu'il sera traité comme du texte. La valeur par défaut est YES. **Remarque :** Pour assurer la compatibilité avec les versions antérieures, vous pouvez remplacer YES par TRUE ou 1 et NO par FALSE ou 0. Ces valeurs étant cependant déconseillées, ne les utilisez pas dans les nouvelles pages.
propname=value	Indique que la propriété propname doit avoir la valeur spécifiée. Pour accéder à cette valeur de propriété dans le fichier inséré, ajoutez le préfixe $prop à propname. Par exemple, la spécification suivante permet au fichier inséré de désigner $prop.menubar : <PDM_INCLUDE … menubar=no> Les propriétés globales peuvent aussi être spécifiées dans le fichier web.cfg. Pour plus d'informations sur le fichier web.cfg, reportez-vous au *Manuel d'administration*. **Remarque** : Pour assurer la compatibilité avec les versions précédentes, vous pouvez référencer les valeurs de propriété spécifiées dans <PDM_INCLUDE> sans le préfixe « prop. », sous la forme $propname. Cette notation étant cependant déconseillée, ne l'utilisez pas dans les pages nouvelles.

PDM_JSCRIPT : Inclure sous conditions un fichier JavaScript

La balise <PDM_JSCRIPT> permet d'inclure sous conditions un fichier JavaScript dans un formulaire. Cette balise prend deux formes :

```
<PDM_JSCRIPT file=xxxx.js [include=yes|no]>
```

Pdm_jscript avec file=xxx.js spécifie que le fichier JavaScript xxx.js est requis par ce formulaire. Le moteur Web ajoute le fichier à une liste de fichiers JavaScript requis par le formulaire. Le traitement de la balise intervient lors de l'analyse du formulaire, sans aucune incidence de la part de pdm_if. C'est-à-dire qu'une balise pdm_jscript qui référence un fichier ajoute ce fichier à la liste des fichiers JavaScript si elle intervient n'importe où dans le fichier ou dans un fichier inclus, ou encore dans une macro.

L'argument facultatif *include=no* peut être spécifié pour indiquer au moteur Web d'ignorer la balise. Cet argument fournit le traitement conditionnel de la balise, et il est surtout utile lorsque la balise est invoquée dans une macro. Par exemple, la macro dtlTextbox spécifie :

```
<PDM_JSCRIPT file=spellcheck.js include=&{spellchk}>
```

Ceci indique qu'un formulaire contenant une macro dtlTextbox qui spécifie spellchk=yes requiert le fichier JavaScript spellcheck.js.

La seconde forme de la balise pdm_jscript est la suivante :
<PDM_JSCRIPT insert=here>

Pdm_jscript avec insert=here demande au moteur Web d'insérer des balises <script> HTML standard pour tous les fichiers JavaScript requis. Le moteur Web traite la balise durant la phase de génération HTML ; elle est donc concernée par pdm_if. Une balise pdm_jscript avec insert=here fait partie de std_head_include.htmpl ; elle est donc présente dans pratiquement tous les formulaires.

Remarque : Le moteur Web insère des balises de script uniquement la première fois qu'il rencontre pdm_jscript insert=here.

PDM_LINK : Créer un lien hypertexte appelant une opération HTMPL

Les balises <PDM_LINK> et </PDM_LINK> peuvent être ajoutées dans n'importe quel modèle HTML d'interface Web pour créer un lien qui appelle une opération HTMPL. La balise <PDM_LINK> génère la balise HTML <a href=...> standard et possède des arguments similaires, à la différence près qu'elle autorise la spécification d'une opération CA SDM à la place d'une URL.

Le format est le suivant, *opération* correspondant à l'une des opérations prises en charge (page 459) :

<PDM_LINK OP=*opération*> ... </PDM_LINK>

Exemple :

```
<PDM_LINK OP=MENU> Menu </PDM_LINK>
<PDM_LINK OP=CREATE_NEW FACTORY=cr> Soumettre la demande client </PDM_LINK>
<PDM_LINK OP=LOGOUT> Déconnexion </PDM_LINK>
```

PDM_LIST : Mettre en forme une liste de lignes d'une base de données

Les balises <PDM_LIST> et </PDM_LIST> délimitent les sections répétitives de code HTML pour une sortie multi-enregistrement. Toutes les opérations qui se trouvent entre <PDM_LIST> et </PDM_LIST> sont répétées une fois pour chaque enregistrement de la sortie. Il existe deux types de balises PDM_LIST :

- Listes tirées d'un attribut d'objet qui implique une liste. Par exemple, l'attribut propriétés de l'objet demande est la liste des propriétés associées à cet appel. Ce type de balise PDM_LIST comporte toujours une propriété SOURCE.
- Listes comportant une clause WHERE explicite. Ce type de balise PDM_LIST comporte toujours une propriété WHERE.

Un attribut d'objet <PDM_LIST> accepte les propriétés suivantes :

Propriété	description
ESC_STYLE=**NONE** | C | HTML | JS | JS2 | URL	Spécifie le type de « traitement » appliqué au texte formaté. Les valeurs valides sont : **NONE** Paramètre par défaut. Aucun traitement spécial n'est appliqué à aucun caractère du corps du contenu. **C** Un traitement spécial est appliqué aux caractères ', ", \, \r, ' et \n, qui ont une signification dans les programmes C. Ces caractères seront ignorés. **HTML** Un traitement spécial est appliqué aux caractères suivants, qui ont une signification dans le texte HTML : & devient & ' devient ' " devient " < devient < > devient %gt; **JS** Un traitement spécial est appliqué aux caractères suivants, qui ont une signification dans le texte JavaScript : ' devient %27 " devient %22 / devient %2F \ devient %5C \r devient %0D \n devient %0A **JS2** Identique à JS, mais aucun traitement spécial n'est appliqué au caractère /, et un traitement spécial est appliqué à deux caractères supplémentaires : - % devient %25 - Les sauts de ligne portent le suffixe %0A **URL** Convertit tous les caractères autres que les lettres, les chiffres et « @*-_.#' en '%xx », où xx est le codage hexadécimal du caractère converti.
LENGTH=*nn*	Spécifie le nombre de lignes de la sortie (par défaut, toutes les lignes).
PREFIX=*préfixe*	Spécifie le préfixe des références aux attributs des enregistrements de la liste. Ceux-ci sont référencés sous la forme *$prefix.attr_name* dans le texte situé entre les balises <PDM_LIST> et </PDM_LIST>. La propriété PREFIX est facultative dans une liste de variables d'objet. Si vous ne définissez pas PREFIX, la valeur de SOURCE est également utilisée comme préfixe.

Propriété	description
SEARCH_TYPE=DISPLAY| **GET_DOB**	Spécifie la méthode que le serveur doit utiliser pour générer le formulaire de liste : DISPLAY Spécifie que le serveur doit émettre une seule requête pour l'intégralité du formulaire GET_DOB Spécifie que le serveur doit émettre des requêtes distinctes pour chaque ligne du formulaire Le choix a des répercussions sur les performances de la liste et dépend de la complexité de la liste (nombre de jointures requises pour l'afficher) ainsi que des caractéristiques de votre SGBD. Les performances de GET_DOB sont plus prévisibles que celles de DISPLAY, et il s'agit de la propriété par défaut.
SORT=*nom-index*	Spécifie le nom de l'index à utiliser pour le tri. La valeur par défaut de cet argument est DEFAULT (correspond au premier index de tri pour le sous-objet sous-jacent).
SOURCE=*source*	Spécifie la variable d'objet définissant cette liste. Ce champ est obligatoire. Ne placez aucun signe dollar ($) devant *source* dans l'instruction PDM_LIST proprement dite. Si la propriété PREFIX n'est pas spécifiée, *source* est également utilisé comme préfixe pour les références aux attributs des enregistrements de la liste, dans les références sous la forme *$source.attr_name*. Quand elle est utilisée dans une référence, *source* doit être précédé du signe dollar.
START=*nn*	Spécifie la première ligne de sortie (zéro, par défaut).

Exemple :

```
<table border>
<tr>
<th>Numéro de la demande de changement enfant</th>
<th>Résumé</th>
</tr>
<PDM_LIST SOURCE=args.children>
<tr>
<td>$args.children.chg_ref_num</td>
<td>$args.children.summary</td>
</tr>
</PDM_LIST>
</table>
```

Aucun préfixe n'ayant été spécifié, les références aux attributs des enregistrements répertoriés sont précédées du préfixe $args.children, qui est la valeur source.

Une clause WHERE PDM_LIST accepte les propriétés suivantes :

Propriété	description
FACTORY=*nom*	Spécifie la classe d'objets pour la recherche. Cette propriété est obligatoire.
LENGTH=*nn*	Spécifie le nombre de lignes de la sortie (par défaut, toutes les lignes).
ORDER_BY=*nom-attr*	Spécifiez le nom de l'attribut à utiliser pour le tri. Vous pouvez préciser le modificateur DESC (descendant) ou ASC (ascendant).
PREFIX=*préfixe*	Spécifie le préfixe des références aux attributs des enregistrements de la liste. Ceux-ci sont référencés sous la forme *$prefix.attr_name* dans le texte situé entre les balises <PDM_LIST> et </PDM_LIST>. La propriété PREFIX est obligatoire dans une liste de clauses WHERE.
START=*nn*	Spécifie la première ligne de sortie (zéro, par défaut).
WHERE=*clause WHERE*	Spécifiez la clause WHERE de la recherche. Elle peut contenir des attributs (séparés par des points). Cette propriété est obligatoire.

Par exemple :

```
<table>
<tr>
<th>Numéro de la demande de changement enfant</th>
<th>Résumé</th>
</tr>
<PDM_LIST PREFIX=list FACTORY=chg WHERE="status = 'OP'">
<tr>
<td>$list.chg_ref_num</td>
<td>$list.summary</td>
</tr>
</PDM_LIST>
</table>
```

PDM_MACRO : Insérer du texte à partir d'un fichier de macro

La balise <PDM_MACRO> permet d'insérer un fichier de macro dans un fichier HTMPL. Ses fonctionnalités sont similaires à celles de la balise PDM_INCLUDE, à deux importantes différences près :

- Un fichier inséré par une balise PDM_MACRO comprend une liste d'arguments formels composée d'arguments obligatoires et d'arguments dotés des valeurs par défaut.
- Un fichier inséré par une balise PDM_MACRO provient toujours du répertoire spécifié pour la propriété de configuration MacroPath, quel que soit le type d'accès de l'utilisateur actuel.

NAME=*nom_macro*

(Obligatoire) Spécifie la macro à insérer. Le moteur Web ajoute le suffixe ".mac" et recherche le fichier dans le chemin spécifié par la propriété du fichier de configuration MacroPath.

D'autres propriétés peuvent être obligatoires, en fonction de la macro insérée. Un fichier de macro se présente généralement comme suit :

```
commentaires
#args
name1 [= value1]
name2 [= value2]
...
#data
data to insert
```

Le tableau suivant explique l'organisation du fichier, ligne par ligne :

- **comments** : les seules instructions valides dans une macro avant l'instruction #args sont les commentaires. Les commentaires sont signalés par le signe # ou les signes // comme premiers caractères autres que des espaces.
- **#args** : doit être codé exactement de la manière indiquée, avec le signe # dans la colonne un et aucune autre information sur la ligne. Cette instruction commence la section args qui peut contenir des définitions des arguments et des commentaires.
- **name [= value]** : définit un argument pour la macro. Seuls les arguments mentionnés explicitement dans la section args sont valides pour la macro. Une valeur spécifiée pour un argument dans la section args est la valeur par défaut de cet argument. Les arguments sans valeur par défaut sont obligatoires. Ils doivent être fournis par l'appelant dans l'instruction <PDM_MACRO> proprement dite.
- **#data** : doit être codé exactement de la manière indiquée, avec le signe # dans la colonne un et aucune autre information sur la ligne. Cette instruction marque le début de la section données, qui fait partie de la macro insérée dans le fichier à l'aide PDM_MACRO. Tout ce qui se trouve dans la section data est inséré dans le fichier appelant, y compris les lignes de commentaires situées avant la section data.
- **data to insert** : données à insérer dans le fichier appelant. Ces données peuvent contenir des références à des arguments sous la forme suivante :
- **&{arg_name}** : ces références sont remplacées par la valeur de l'argument fourni par l'appelant ou par la valeur par défaut si l'appelant n'a pas fourni de valeur.

Le moteur Web ne lit normalement un fichier de macro qu'une seule fois, lors de sa première utilisation, puis stocke la macro analysée dans sa mémoire. Ceci améliore les performances mais peut constituer un inconvénient si vous développez une macro. Utilisez la propriété du fichier de configuration SuppressMacroCache pour éviter ce comportement et amener le moteur Web à rejeter toutes les macros en mémoire chaque fois qu'il commence à traiter un nouveau formulaire.

Pour commenter des balises PDM_MACRO

Pour commenter des balises <PDM_MACRO>, entrez un point d'exclamation devant le P, comme suit : <!PDM_MACRO>. Pour que le navigateur ne puisse pas traiter la partie commentée du formulaire, placez <PDM_IF 0> avant la balise <!PDM_MACRO>, et </PDM_IF> après la ligne que vous avez commentée.

Exemple :

```
<PDM_IF 0>

<!PDM_MACRO NAME=dtlDropdown hdr="Etat" attr=status lookup=no
evt="onBlur=\\\"detailSyncEditForms(this)\\\"">
<!PDM_MACRO NAME=dtlDropdown hdr="Priorité" attr=priority lookup=no
evt="onBlur=\\\"detailSyncEditForms(this)\\\"">

</PDM_IF>
```

Macros prédéfinies utilisées par l'outil WSP

CA SDM inclut un nombre de macros prédéfinies. La plupart de ces macros insèrent du texte JavaScript destiné à créer un élément dans un formulaire Web. Utilisez l'Outil de conception Web pour créer et modifier des formulaires à l'aide de ces macros.

Macros des formulaires détaillés

La liste suivante décrit les macros de formulaires détaillés :

button

Insère un bouton dessiné.

dtlCheckbox

Insère une case à cocher sur un formulaire détaillé.

dtlDate

Insère un champ de date sur un formulaire détaillé.

dtlDateReadonly

Insère un champ de date en lecture seule sur un formulaire détaillé.

dtlDropdown

Insère une liste déroulante sur un formulaire détaillé.

dtlEnd

Termine un formulaire détaillé.

dtlEndTable

Termine une table dans un formulaire détaillé.

dtlForm

Débute un formulaire détaillé.

dtlHTMLEditBox

Insére un champ de formulaire détaillé qui est une zone de texte contenant un éditeur HTML.

dtlHier

Insère un champ de formulaire détaillé qui est une zone de texte validée dans une table externe avec une recherche hiérarchique.

Important : Nous recommandons de ne pas modifier la macro dtlHier en dtlLookup dans le fichier HTMPL. Utilisez plutôt l'option suppress_web_hier_search du gestionnaire d'options de sorte que l'exécution automatique fonctionne correctement.

dtlLookup

Insère un champ de formulaire détaillé qui est une zone de texte validée dans une table externe.

dtlLookupReadonly

Insère un champ de formulaire détaillé qui est un lien hypertexte en lecture seule vers une table externe.

dtlReadonly

Insère un champ de texte en lecture seule sur un formulaire détaillé.

dtlStart

Débute la première table dans un formulaire détaillé.

dtlStartExpRow

Débute une ligne susceptible d'être développée sur un formulaire détaillé.

dtlStartRow

Débute une ligne normale sur un formulaire détaillé.

dtlTextbox

Insère une zone de texte sur un formulaire détaillé.

contactLookup

La macro contactLookup crée une recherche de contact. Cette macro comporte les arguments suivants :

```
contactLookup("&{header}","&{frameName}","&{factory}","&{lookupName}");
```

header

Identifie l'en-tête de la recherche.

frameName

(Obligatoire) Identifie le nom du formulaire.

Sous-objet

Spécifie le sous-objet.

Valeur par défaut : agt

lookupName

(Obligatoire) Identifie le nom de la recherche.

Vous pouvez aussi activer et désactiver cet élément en procédant comme suit :

```
contactLookupDisable( Name, bDisable )
```

bDisable=

- true

  Désactive l'élément.

- false

  Active l'élément.

dtlCheckboxReadonly

La macro dtlCheckboxReadonly spécifie un champ de case à cocher en lecture seule sur un formulaire de détail HTMPL. La macro contient les arguments suivants :

```
detailCheckboxReadonly("&{hdr}","&{attr}",&{colspan},"$args.&{attr} "&{on}
"&{off}) ;
```

hdr

Indique le texte de l'en-tête.

Valeur par défaut : $args.&{attr}.DISPLAY_NAME

attr

(Obligatoire) Spécifie le nom de l'attribut.

on = X

Spécifie la valeur affichée sur le formulaire en lecture seule quand ce champ est coché.

off = ""

Spécifie la valeur affichée sur le formulaire en lecture seule quand ce champ n'est pas coché.

colspan = 1

Spécifie le nombre de colonnes dans le formulaire.

Sur les deux formulaires en lecture seule et de modification, ce champ s'affiche selon ce que spécifient les arguments on et off.

Remarque : Cette macro est similaire à dtlCheckbox.mac, à ceci près qu'elle est toujours en lecture seule, même en mode Edition.

Macros des formulaires de liste

lsCol

Spécifie une colonne dans un formulaire de liste.

lsEnd

Débute la portion liste d'un formulaire de liste.

lsStart

Débute la portion liste d'un formulaire de liste.

lsWrite

Insère du texte dans la section de répétition d'un formulaire de liste.

sfDate

Insère un champ de date dans un filtre de recherche.

sfDropdown

Insère une liste déroulante dans un filtre de recherche.

sfEnd

Termine un filtre de recherche.

sfHier

Insère un champ de filtre de recherche qui est une zone de texte validée dans une table externe avec une recherche hiérarchique.

sfLookup

Insère un champ de filtre de recherche qui est une zone de texte validée dans une table externe.

sfStart

Débute un filtre de recherche.

sfStartRow

Débute une ligne dans un filtre de recherche.

sfTextbox

Insère une zone de texte dans un filtre de recherche.

Macros des barres de menus

La liste suivante décrit les macros Menubar :

endMenu

Termine un menu dans une barre de menus.

menuItem

Définit un élément global dans un menu.

endMenubar

Termine une barre de menus.

menuItemLocal

Définit un élément d'un menu appelé dans le contexte de la fenêtre actuelle.

menubarItem

Définit un menu dans une barre de menus.

startMenu

Débute un menu dans une barre de menus.

startMenubar

Débute une barre de menus.

PDM_NOTEBOOK : Créer un carnet

Plusieurs formulaires de l'interface analyste de CA SDM utilisent des onglets imbriqués (carnets). Les onglets imbriqués affichent plusieurs groupes de champs dans la même zone physique de l'écran, un seul groupe s'affichant à la fois. L'utilisateur sélectionne le groupe de champs à afficher en cliquant sur l'onglet approprié en haut du carnet ou en appuyant sur la combinaison de touches d'accès Alt+*n*, *n* correspondant au numéro de l'onglet. Par exemple, le formulaire Détail de la demande client (detail_iss.htmpl) utilise un carnet. Nous vous conseillons d'utiliser l'outil WSP pour modifier le contenu des carnets ou insérer un carnet dans un formulaire qui n'en contient encore aucun.

La balise suivante marque la fin d'un carnet :

```
<PDM_MACRO name=endNotebook>
```

PDM_PRAGMA : Spécifier les informations du serveur

La balise <PDM_PRAGMA> permet de spécifier les informations utilisées par le moteur Web, telles que la version d'un formulaire. Elle ne génère aucun code HTML, et elle peut être placée n'importe où dans un formulaire. Les arguments possibles sont les suivants :

Argument	description
RELEASE=valeur	Spécifie le numéro de version d'CA SDM correspondant à ce formulaire. Cette valeur est "110" sur tous les formulaires d'Unicenter Service Desk r11.0. Elle est accessible, à l'intérieur du formulaire, dans la variable $prop.release.
SITEMOD=valeur	Spécifie une chaîne définie par le site identifiant les modifications apportées au formulaire. Elle est accessible, à l'intérieur du formulaire, dans la variable $prop.sitemod.
VERSION=valeur	Spécifie une chaîne définie par CA Technologies identifiant le numéro de version de ce formulaire. Elle est accessible, à l'intérieur du formulaire, dans la variable $prop.version.
OVERIDE=YES|**NO**	Spécifie si les valeurs de cette instruction PDM_PRAGMA remplacent ou non celles des instructions PDM_PRAGMA précédentes.

CA Technologies utilise les instructions PDM_PRAGMA pour donner des informations sur la version du formulaire. Tous les formulaires d'Unicenter Service Desk r11.0 incluent l'instruction PDM_PRAGMA suivante :

```
<PDM_PRAGMA RELEASE=110>
```

Qui plus est, le formulaire std_head.htmpl inclut l'instruction JavaScript suivante :

```
cfgFormRelease = “$prop.release” - 0;
```

L'instruction PDM_PRAGMA et la variable cfgFormRelease permettent à l'interface Web de CA SDM de faire la distinction entre les formulaires Unicenter Service Desk r11.0 et ceux des versions antérieures. Les versions antérieures à la version d'Unicenter Service Desk r6.0 ne prennent pas en charge l'instruction PDM_PRAGMA.

Normalement, seules les instructions PDM_PRAGMA dans le fichier du plus haut niveau d'un formulaire (c'est-à-dire, un fichier ne provenant pas de PDM_INCLUDE) sont utilisées pour définir $prop.release, $prop.sitemod et $prop.version. En outre, une instruction PDM_PRAGMA ne remplacera pas une valeur non vide définie par une instruction PDM_PRAGMA antérieure. Vous pouvez définir OVERRIDE=YES pour spécifier qu'une instruction PDM_PRAGMA peut remplacer des instructions PDM_PRAGMA précédentes ou qu'une instruction PDM_PRAGMA d'un fichier inséré peut être utilisée.

PDM_SCOREBOARD : Générer une arborescence du tableau de résultats

La balise <PDM_SCOREBOARD> permet de générer le tableau de résultats placé sur la gauche du formulaire principal. Il accepte la propriété suivante :

TARGET=*valeur*

Spécifie le nom du cadre cible pour les listes demandées en cliquant sur un noeud du tableau de résultats. Ces listes sont chargées dans la cible spécifiée (l'une des valeurs prises en charge pour l'attribut cible d'un lien). La valeur par défaut est *_self* (fenêtre contenant la balise PDM_SCOREBOARD).

Tous les formulaires HTMPL contenant une balise <PDM_SCOREBOARD> doivent également comprendre le fichier JavaScript fldrtree.js. Cette opération peut être effectuée à l'aide de l'instruction suivante dans la section <HEAD> du formulaire :

```
<SCRIPT LANGUAGE="JavaScript" SRC="$CAisd/CAisd/fldrtree.js"></SCRIPT>
```

Il est également recommandé d'insérer un lien appelé scoreboard_asof_data pour afficher la date d'effet des valeurs dans l'arborescence. Reportez-vous à l'exemple d'utilisation de cette balise donné dans la section consacrée au fichier distribué scoreboard.htmpl.

Les requêtes incluses dans le tableau de résultats sont définies par le contenu de la table User_Query (nom d'objet usq) de l'utilisateur actuel. Un enregistrement de cette table définit chaque ligne de l'arborescence (dossier ou nœud).

A l'origine, la table User_Query des utilisateurs ne comporte aucune entrée. Chaque utilisateur sans entrée User_Query reçoit l'ensemble par défaut des requêtes de tableau de résultats associé à son type d'accès. Un utilisateur disposant des droits administratifs peut également personnaliser le tableau de résultats par défaut pour un type d'accès.

PDM_SET : Définir la valeur d'une variable serveur

La balise <PDM_SET> permet d'affecter une valeur à une variable serveur. Elle présente la syntaxe suivante :

`<PDM_SET arg.`*`name`*`[+]=value>`

arg

(Obligatoire) Spécifie le type de variable, et il doit s'agir d'arg dans le cadre d'une utilisation normale.

Remarque : Il n'y a pas de caractère $.

Nom

(Obligatoire) Spécifie le nom de la variable.

+

(Facultatif) Spécifie que la valeur doit être ajoutée à la valeur existante de la variable. Il ne peut y avoir d'espaces ni avant ni après.

=

(Obligatoire) Ce signe doit être spécifié tel qu'il apparaît, sans aucun espace avant ou après.

Valeur

(Obligatoire) Spécifie le texte à affecter ou à ajouter à la variable.

La balise PDM_SET peut également être utilisée dans la phase de préprocesseur pour créer ou mettre à jour une variable de préprocesseur.

Informations complémentaires :

Prétraitement du moteur Web (page 480)

PDM_TAB : Créer un onglet dans un carnet

La balise <PDM_MACRO name=startNotebook hdr=cng_nb> permet de définir un onglet de carnet. Nous vous conseillons d'utiliser l'outil WSP pour modifier le contenu des carnets ou insérer un carnet dans un formulaire qui n'en contient encore aucun.

PDM_WSP : Contrôle de l'aperçu de l'outil de conception Web

La balise <PDM_WSP> permet de contrôler la fonctionnalité d'aperçu de l'outil WSP. Elle ne génère aucun code HTML, et elle peut être placée n'importe où dans un formulaire.

Par défaut, l'outil WSP détermine la méthode d'affichage de l'aperçu d'un formulaire en examinant son nom :

- Pour les formulaires détaillés (noms du formulaire detail_*factory*.htmpl), l'outil WSP affiche le formulaire en mode Edition, avec les données de la dernière ligne créée de la table appropriée. S'il n'existe aucune donnée que vous êtes autorisé à afficher dans la table, l'outil WSP affiche le formulaire configuré pour créer une ligne. En général, la mise à jour de la base de données est interdite dans les sessions d'aperçu l'outil WSP. L'outil WSP affiche les formulaires en mode édition pour permettre d'afficher l'aperçu de toutes les fonctions. CA SDM ignore cependant une demande Enregistrer dans une session d'aperçu en lecture seule. Le moteur Web remplace l'intitulé du bouton Enregistrer par la mention Pas d'enregistrement ; il s'agit là d'un rappel visuel de cette interdiction.
- Pour les formulaires de liste (noms du formulaire list_*factory*htmpl), l'outil WSP affiche le formulaire sous forme de liste, celle-ci présentant les données issues de la dernière ligne créée de la table appropriée. S'il n'existe aucune donnée que vous êtes autorisé à afficher dans la table, l'outil WSP affiche le formulaire en mode de recherche, le filtre étant ouvert.
- Pour les autres formulaires, l'outil WSP affiche simplement le formulaire sans aucun contexte de base de données.

Vous pouvez modifier ce comportement par défaut en insérant une balise PDM_WSP n'importe où dans le formulaire. Par exemple, vous pouvez afficher un formulaire de carnet sur son formulaire détaillé associé, ou fournir des arguments prérequis pour les formulaires normalement appelés avec un environnement fourni par un autre formulaire. Les arguments possibles sont les suivants :

Propriété	**description**
FACTORY=*valeur*	Spécifie le sous-objet Moteur d'objets utilisé par ce formulaire.
PREVIEW=*nom*.htmpl | *valeur* | no	Spécifie l'URL d'aperçu. Il peut s'agir d'un nom de fichier HTMPL sous la forme xxxx.htmpl, d'une URL CA SDM (utilisée telle quelle si elle commence par « OP= ») ou du mot-clé « non » indiquant qu'il est impossible d'afficher un aperçu du formulaire. Il est possible de modifier une valeur ne commençant pas par OP=, en remplaçant une référence sous la forme {*factory*} ou {*factory*:} par l'ID ou l'ID persistant (respectivement) de la ligne la plus récente du sous-objet référencé que l'utilisateur actuel est autorisé à voir.
WHERE=*valeur*	Spécifie une clause Where permettant de rechercher une ou plusieurs lignes représentatives à afficher sur le formulaire prévisualisé.

Propriété	description
MODE=*valeur*	Spécifie l'emplacement de l'URL créée. Peut être ce qui suit : ■ GENERALITES. Format général. Détermine le mode en examinant l'argument d'aperçu : detail_xxxx.htmpl - READONLY list_xxxx.htmpl - LIST any other - GRONK ■ READONLY. Fichier de détail en mode lecture seule. ■ EDIT. Fichier de détail en mode édition. ■ LIST. Fichier de liste. ■ GRONK. Fichier non spécifié. Dans ce cas, réinitialisez le fichier.

Variables serveur

Des informations CA SDM sont incluses dans le modèle HTML à l'aide de variables commençant par le symbole du dollar ($). Chaque page est créée à l'aide des variables décrites dans le modèle. Ces variables sont placées dans la page ou dans des instructions conditionnelles :

- Variables simples
- Variables de propriété
- Variables d’environnement
- Variables d'objet métier
- Variables de liste

Variables simples

Les variables simples spécifient des indicateurs transmis à la page Web. Pour accéder à une variable simple, entrez son nom précédé du symbole du dollar ($). La valeur de la variable devient alors disponible. Par exemple, $CAisd et $cgi sont deux variables simples. Insérée dans un modèle, la variable $CAisd se substitue au répertoire d'installation principal du serveur Web de CA SDM, tandis que $cgi correspond à l'adresse URL du programme pdmweb.exe. Les variables simples figurent dans la section supérieure du fichier HTMPL qui les utilise.

La liste suivante répertorie les variables que vous pouvez utiliser dans tous les fichiers HTMPL :

$ACCESS.*groupe*

L'objet de droit d'accès utilisateur contient les paramètres de droit d'accès au groupe fonctionnel *groupe* pour l'utilisateur actuellement connecté. Par exemple, $ACCESS.admin contient la valeur de droit d'accès pour le groupe fonctionnel admin. Un droit peut prendre les valeurs suivantes :

- 0-AUCUN ACCES
- 1-AFFICHAGE
- 2-MODIFICATION

Cette variable n'est pas disponible dans le formulaire de connexion.

$cgi

Adresse URL du programme pdmweb.exe.

$cst

Objet de données pour l'utilisateur actuellement connecté. Cette variable n'est pas disponible dans le formulaire de connexion. Vous pouvez indiquer des attributs de cet objet sous la forme $cst.*nom-attr* (par exemple, $cst.first_name).

$CAisd

URL du répertoire d'installation principal du serveur Web CA SDM.

$MachineName

Le MachineName défini dans le fichier web.cg.

Remarque : Pour plus d'informations sur le fichier web.cfg, reportez-vous au *Manuel d'administration*.

$ProductName

Nom du produit tel qu'il est défini dans le fichier NX.env.

$SESSION

L'objet de session enregistre toutes les variables de session y compris l'ID de session ($SESSION.SID) et toutes les variables définies dans le fichier web.cfg.

Remarque : Pour plus d'informations sur le fichier web.cfg, reportez-vous au *Manuel d'administration*.

$USER_STATE

Informations d'état définies par l'utilisateur.

Variables de propriété

Les variables de propriété représentent une propriété du fichier de configuration web.cfg. Vous pouvez accéder à une entrée dans le fichier web.cfg (y compris celles définies par l'utilisateur) dans un fichier de modèle HTML en lui ajoutant le préfixe "$prop."

Par exemple, la ligne suivante de web.cfg spécifie le nombre d'entrées affichées dans une page d'un formulaire de liste, comme suit :

```
ListPageLength 10
```

Pour désigner cette variable dans un modèle HTML, utilisez la spécification suivante :

```
$prop.ListPageLength
```

Si vous utilisez la balise spéciale <PDM_INCLUDE> pour insérer un autre fichier dans un modèle, vous pouvez spécifier des propriétés supplémentaires en tant qu'attributs de la balise <PDM_INCLUDE>. Vous pouvez désigner ces propriétés dans le fichier inséré de la même manière que pour les propriétés web.cfg. Une propriété définie en tant qu'attribut <PDM_INCLUDE> et portant le même nom qu'une propriété de web.cfg remplace cette dernière dans le fichier inséré.

Par exemple, la balise <PDM_INCLUDE> suivante crée la propriété $prop.menubar, qui peut être indiquée dans le fichier std_body.htmpl :

```
<PDM_INCLUDE FILE=std_body.htmpl menubar=no>
```

Remarque : Vous pouvez appeler la propriété de fichier de configuration *xxx* de deux façons : $prop.*xxx* ou *$SESSION.xxx*. Les deux renvoient la même valeur. La syntaxe $prop.*xxx* est toutefois préférable, car elle entraîne moins de surcharge pour le serveur.

En plus des propriétés de web.cfg, $prop vous permet d'accéder à d'autres propriétés prédéfinies Il s'agit de :

$prop.browser

Chaîne identifiant le navigateur utilisé. Il s'agira de "IE" pour Internet Explorer.

$prop.combo_name

Chaîne contenant le nom de l'utilisateur actuel, sous la forme « nom, prénom second_prénom ».

$prop.factory

Chaîne contenant le sous-objet associé au formulaire actuel, par exemple "cr" pour les demandes ou "iss" pour les demandes client.

$prop.FID

Chaîne contenant l'ID numérique du formulaire actuel.

$prop.form_name

Chaîne contenant le nom du modèle HTML actuel, dans le formulaire *xxx*.htmpl.

$prop.form_name_1

Chaîne contenant la partie du nom de formulaire placée avant le premier trait de soulignement. Par exemple, pour le formulaire detail_chg_edit.htmpl, form_name_1 correspond à « detail ».

$prop.form_name_2

Chaîne contenant la partie du nom de formulaire placée après le premier trait de soulignement et avant le dernier (ou avant le point). Par exemple, pour le formulaire detail_chg_edit.htmpl, form_name_2 correspond à « chg ».

$prop.form_name_3

Chaîne contenant la partie du nom de formulaire placée entre le dernier trait de soulignement et le point. Par exemple, pour le formulaire detail_chg_edit.htmpl, form_name_3 serait "edit". Pour le formulaire détaillé de la combinaison, qui a un nom de fichier de type detail_*xxx*.htmpl, $prop.form_name_3 est défini sur le mode actuel ou sur "ro" ou "edit".

$prop.release

Chaîne contenant le niveau de la version du formulaire. L'instruction PDM_PRAGMA contient plus de détails sur cette propriété.

$prop.SID

Chaîne contenant l'ID numérique de la session actuelle.

$prop.sitemod

Chaîne contenant le nom de modification défini par le site du formulaire. L'instruction PDM_PRAGMA contient plus de détails sur cette propriété.

$prop.user_type

Chaîne contenant le texte « analyste », « client », « employé » ou « invité ».

$prop.version

Chaîne contenant la version du formulaire. L'instruction PDM_PRAGMA contient plus de détails sur cette propriété.

Informations complémentaires :

PDM_PRAGMA : Spécifier les informations du serveur (page 449)

Variables d’environnement

Les variables d'environnement correspondent à une entrée du fichier de configuration NX.env. Pour désigner une entrée de ce type dans un modèle HTMPL, ajoutez-lui le préfixe $env.

Par exemple, l'une des lignes de NX.env, qui spécifie le nom d'hôte du serveur CA SDM se présente comme suit :

```
@NX_SERVER=nom_hôte
```

Pour désigner cette variable dans un modèle HTML, utilisez la spécification suivante :

```
$env.NX_SERVER
```

Variables d'objet métier

Les variables d'objet métier représentent un objet CA SDM, par exemple une demande client ou une demande. Pour accéder à un objet, indiquez le nom de la variable suivi d'un point (.) et des noms d'attributs à afficher. Par exemple, pour une demande client dont l'objet est conventionnellement représenté par la variable args, vous pouvez afficher la description, la date d'ouverture, le numéro de téléphone de la personne assignée, le nombre d'activités pour la demande client et la description de la première activité, comme suit :

```
$args.description
$args.open_date
$args.assignee.phone_number
$args.act_log.length
$args.act_log.0.description
```

Vous pouvez délimiter le nom de la variable par des accolades s'il n'est pas déjà entouré par des espaces. Par exemple, $foo bar et ${foo}bar sont deux syntaxes valides. Vous pouvez également utiliser la variable args pour accéder à des valeurs autres que des valeurs d'attributs (par exemple, $args.KEEP.*nom* comme décrit dans la section Opérations prises en charge (page 459)).

Il est possible qu'une variable autre qu'un attribut ne soit pas définie. Par exemple, il peut être possible d'obtenir un formulaire à partir de deux emplacements, dont un seul d'entre eux fournit une valeur pour $args.KEEP.foo. Vous pouvez indiquer une valeur par défaut pour une référence $args à l'aide de la syntaxe suivante, la chaîne après le signe deux-points remplaçant la référence si *variable* n'est pas définie :

```
${args.variable:default}
```

Variables de date de fuseau horaire

Les variables de date de fuseau horaire sont une forme particulière de variables d'objet métier. Elles permettent de convertir les dates universelles (UTC) numériques en dates de type chaîne ajustées au fuseau horaire du navigateur de l'utilisateur. Les dates numériques sont représentées par la variable suivante :

`$args.`*`nom_attr`*`_INT_DATE`

Exemple : $args.open_date_INT_DATE

Variables de données du sous-objet

Les variables de données du sous-objet sont une forme particulière de variables d'objet métier. Une variable de données de sous-objet est remplacée par des informations sur un objet référencé. Sept variables de ce type sont disponibles :

$args.*nom_attr*.COMMON_NAME

Nom commun (chaîne lisible à l'extérieur) de la table référencée par l'attribut. Par exemple, dans le formulaire Détail de l'appel, la valeur de $args.assignee.COMMON_NAME est le nom combiné de la personne assignée (« nom, prénom, second prénom »).

$args.attr_name.COMMON_NAME_ATTR

Nom d'attribut du nom commun dans la table référencée par l'attribut. Par exemple, dans le formulaire Détail de l'appel, la valeur de $args.assignee.COMMON_NAME_ATTR est « combo_name ».

$args.FACTORY_*nom_attr*

Nom du sous-objet associé à l'attribut spécifié. Par exemple, dans le formulaire Détail de l'appel, la valeur de $args.FACTORY_assignee est « agt ».

$args.LENGTH_*nom_attr*

Longueur maximale de l'attribut. Par exemple, dans le formulaire Détail de l'appel, la valeur de $args.LENGTH_summary est 240.

$args.*nom_attr*.REL_ATTR

Attr-rel (clé étrangère) de l'attribut. Par exemple, dans le formulaire Détail de l'appel, la valeur de $args.assignee.REL_ATTR est la valeur du champ ID de la personne assignée.

$args.*nom_attr*.REL_ATTR_ATTR

Nom d'attribut de l'attr-rel dans la table référencée par l'attribut. Par exemple, dans le formulaire Détail de l'appel, la valeur de $args.assignee.REL_ATTR_ATTR est « id ».

$args.REQUIRED_*nom_attr*

Chaîne, « 0 » ou « 1 » indiquant si l'attribut référencé est obligatoire.

$args.*nom_attr*.SELECTIONS

Liste de sélections valides pour *nom_attr*. La valeur est une chaîne vide si *nom_attr* n'est pas une référence à une autre table ou si la taille de la table désignée par *nom_attr* est supérieure à la valeur de la propriété SelListCacheMax du fichier de configuration. Sinon, la variable SELECTIONS est une chaîne contenant le nom commun et l'attr-rel de toutes les entrées de la table référencée. Les valeurs successives sont séparées par la chaîne « @,@ », de sorte que la valeur de la variable se présente sous la forme suivante :

"cname1@,@rel_attr1@,@cname2@,@rel_attr2"

$args.*sous-objet*_SEL_UNDER_LIMIT

Chaîne, "0" ou "1", indiquant si le nombre actuel de lignes dans la table correspondant au *sous-objet* est inférieur à la valeur de la propriété SelListCacheMax du fichier de configuration. Cette variable est déconseillée par rapport à la variable SELECTIONS qu'il est préférable d'utiliser dans tous les nouveaux formulaires.

Vous pouvez utiliser les variables de données de sous-objet incluant une référence contenant des points (COMMON_NAME, REL_ATTR et SELECTIONS) avec une référence contenant des points d'une longueur quelconque. Par exemple, dans le formulaire Détail de l'appel, $args.assignee.organization.COMMON_NAME est remplacé par le nom externe de l'organisation de la personne assignée.

Variables de liste

Les variables de liste permettent de répéter des opérations dans les données. Elles sont accessibles à l'aide de balises de liste comme décrit dans PDM_LIST : Mettre en forme une liste de lignes d'une base de données (page 439).

Opérations de serveur prises en charge

Les opérations suivantes sont prises en charge pour vous permettre d'intégrer les pages Web de CA SDM dans vos pages Web :

CREATE_NEW

Fournit une interface générique permettant à l'utilisateur de créer une ligne dans une table spécifiée. Vous devez entrer le nom d'objet. Par défaut, un modèle nommé *detail_xxx*_edit.htmpl est utilisé pour l'objet *xxx*. Vous pouvez remplacer le fichier .htmpl en spécifiant la propriété HTMPL.

Identificateurs obligatoires :

FACTORY=*nom-objet*

Identificateurs facultatifs :

ALG_PRESET=*expression_prédéfinie*
ALG_PRESET_REL=expression_prédéfinie
CREATE_ALG=*type_journal_activité*
HTMPL=zdetailxxx_*sous-objet*.htmpl
KEEP.*nom_attr=valeur*
PRESET=*expression_prédéfinie*
PRESET_REL=*expression_prédéfinie*
SET.*nom_attr=valeur*
use_template=1 | 0 (0 par défaut)

Remarque : Pour que vous puissiez utiliser l'indicateur HTMPL avec CREATE_NEW, le nom du formulaire référencé doit respecter la convention d'affectation de noms zdetailxxx_*sous-objet*.htmpl. Le nom doit commencer par la chaîne « zdetail » puis être suivi de caractères alphanumériques (y compris une chaîne nulle), d'un caractère de soulignement et du nom du sous-objet.

ENDSESSION ou LOGOUT

Termine la session en cours. Il est conseillé d'utiliser l'opération ENDSESSION.

GENERIC_LIST

Fournit une interface générique permettant à l'utilisateur d'afficher une liste à partir d'une table de la base de données. Vous devez entrer le nom d'objet. Par défaut, un modèle nommé list_*xxx*.htmpl est utilisé pour l'objet *xxx*. Vous pouvez remplacer le fichier .htmpl en spécifiant la propriété HTMPL.

Identificateurs obligatoires :

FACTORY=*nom-objet*
KEEP.*nom_attr=valeur*

DISPLAY_FORM

Fournit une interface générique permettant à l'utilisateur d'afficher un formulaire personnalisé.

Identificateurs obligatoires :

HTMPL=*fichier_htmpl*

Remarque : DISPLAY_FORM remplace JUST_GRONK_IT. Les mises en oeuvre existantes peuvent continuer à utiliser JUST_GRONK_IT, qui fonctionne exactement comme DISPLAY_FORM. Il est conseillé d'utiliser l'opération ENDSESSION.

MENU

Affiche la page de menu principale, qu'est définie dans le fichier web.cfg de la propriété Menu.

Identificateurs facultatifs :

HTMPL=*fichier_menu*

fichier_menu correspond au nom d'un fichier de menu principal de remplacement.

PAGE_EXTENSION

Permet à l'administrateur Web de spécifier des extensions supplémentaires pour l'interface.

Identificateurs obligatoires :

NAME=*fichier_html*

fichier_html est l'un des noms de fichier répertoriés dans la directive UserPageExtensions du fichier de configuration.

Identificateurs facultatifs :

REQUIRES_LOGIN=1

S'il est présent, une page de connexion apparaît d'abord si l'utilisateur n'est pas connecté actuellement. S'il est omis ou défini sur zéro, le fichier est affiché sans vérifier si l'utilisateur est connecté actuellement.

RELOG

Affiche la page de connexion.

SEARCH

Fournit une interface générique pour permettre les recherches dans les tables de la base de données. Cette opération suppose qu'un fichier search_*xxx*.htmpl approprié a été créé, *xxx* correspondant au *nom d'objet*, comme défini dans les fichiers .maj du répertoire majic dans bopcfg.

Remarque : Pour de plus amples renseignements, reportez-vous au *Manuel de référence technique de CA SDM*. Par défaut, les résultats de cette recherche sont affichés dans list_*xxx*.htmpl, mais vous pouvez modifier cette option en spécifiant la propriété HTMPL.

Identificateurs obligatoires :

FACTORY=*nom-objet*
QBE.*op.nom_attrib=valeur*

Identificateurs facultatifs :

ALG_PRESET=*expression_prédéfinie*
ALG_PRESET_REL=*expression_prédéfinie*
CREATE_ALG=*type_journal_activité*
HTMPL=*fichier_htmpl_liste*
KEEP.*nom_attr=valeur*

SEC_REFRESH

Actualise les informations d'accès utilisateur à partir du sous-système de sécurité. Pour ce faire, les utilisateurs bénéficiant des droits de modification (pour le groupe fonctionnel admin) sur l'écran de menu ont accès à un lien hypertexte. Après la mise à jour des droits d'accès d'un utilisateur à l'aide du programme de sécurité, cette opération permet d'actualiser les informations d'accès (cette actualisation s'étend à tous les utilisateurs).

Remarque : L'actualisation de la sécurité est un processus asynchrone. Une fois l'actualisation terminée, un message s'affiche dans le journal standard (stdlog).

SET_MENU

Cette opération est identique à l'opération MENU lorsque vous utilisez MENU avec la variable HTMPL, à la différence près qu'elle définit également le formulaire de menu par défaut au formulaire spécifié à l'aide de la propriété HTMPL.

Identificateurs obligatoires :

HTMPL=*fichier_htmpl*

Remarque : La définition de MENU dans le fichier web.cfg sera alors ignorée jusqu'au redémarrage du service Web.

SHOW_DETAIL

Fournit une interface générique permettant à l'utilisateur d'afficher en lecture seule le détail d'une ligne dans une table spécifiée. Le nom d'ID persistant doit être spécifié (il permet de déterminer le nom d'objet). Par défaut, un modèle nommé detail_*xxx*_ro.htmpl est utilisé pour l'objet *xxx*. Vous pouvez remplacer le fichier .htmpl en spécifiant la propriété HTMPL.

Identificateurs obligatoires :

PERSID=*id-persistant*

Identificateurs facultatifs :

ALG_PRESET=*expression_prédéfinie*
ALG_PRESET_REL=*expression_prédéfinie*
CREATE_ALG=*type_journal_activité*
HTMPL=*fichier_htmpl_détail_lecture-seule*

UPDATE

Fournit une interface générique pour modifier une table. L'ID et le nom d'objet doivent être transmis, et un formulaire détaillé susceptible d'être modifié s'affiche pour l'utilisateur. Par défaut, l'utilisateur a un accès exclusif à l'enregistrement pendant deux minutes et est certain que ses modifications seront appliquées si elles sont soumises pendant ce délai.

Identificateurs obligatoires :

PERSID=*id-persistant* ou
SET.id=*id-de-ligne-à-mettre_à_jour* FACTORY=*nom-objet*

Identificateurs facultatifs :

NEXT_PERSID=*id-persistant* (de l'enregistrement à afficher après la mise à jour)
KEEP.*nom_attr=valeur*
KEY.*nom_attr=valeur*
HTMPL=zdetailxxx_*sous-objet*.htmpl

Remarque : Pour que vous puissiez utiliser l'indicateur HTMPL avec UPDATE, le nom du formulaire référencé doit respecter la convention d'affectation de noms zdetailxxx_sous-objet.htmpl. Le nom doit commencer par la chaîne « zdetail » puis être suivi de caractères alphanumériques (y compris une chaîne nulle), d'un caractère de soulignement et du nom du sous-objet.

Remarque : Pour de plus amples renseignements sur le fichier web.cfg, reportez-vous au *Manuel d'administration*.

Variables d'opération

Le tableau suivant répertorie les variables pouvant être définies pour chacune des opérations prises en charge :

Variables	description	Service Opérations
ALG_PRESET ALG_PRESET_REL	Spécifie les valeurs d'un ou plusieurs attributs du journal d'activité créé suite à l'utilisation de la variable CREATE_ALG. Si la variable CREATE_ALG n'est pas spécifiée, les variables ALG_PRESET et ALG_PRESET_REL sont ignorées.	CREATE_NEW SEARCH SHOW_DETAIL
CREATE_ALG	Spécifie le type de journal d'activité à créer en tant qu'effet secondaire de l'opération. Utilisez les variables ALG_PRESET ou ALG_PRESET pour spécifier les valeurs des attributs du nouveau journal d'activité. Le moment de la création du journal d'activité dépend de l'opération, comme suit : **CREATE_NEW** Le journal d'activité est créé lors de la sauvegarde de l'enregistrement. Si le nouvel enregistrement n'est pas enregistré, aucun journal d'activité n'est créé. **SEARCH** Le journal d'activité est créé lors de la sélection d'un enregistrement dans le formulaire de liste. Si l'enregistrement est consulté plutôt que sélectionné (c'est-à-dire, si l'utilisateur sélectionne de façon explicite la commande Affichage dans le menu contextuel du formulaire de liste), aucun journal d'activité n'est créé. **SHOW_DETAIL** Le journal d'activité est créé avant l'affichage de l'enregistrement.	CREATE_NEW SEARCH SHOW_DETAIL
FACTORY	Spécifie la classe d'objets à rechercher, à créer ou à mettre à jour. Vous pouvez utiliser n'importe quel nom spécifié comme OBJECT dans les fichiers *.maj figurant dans le répertoire $NX_ROOT/bopcfg, comme indiqué dans le Manuel de référence technique de CA SDM.	CREATE_NEW GENERIC_LIST SEARCH UPDATE
HTMPL	Permet à l'auteur HTMPL d'ignorer les conventions d'affectation des noms de modèles par défaut et de spécifier explicitement le fichier HTMPL à afficher à la place du modèle par défaut. **Remarque** : Lorsque l'indicateur HTMPL est utilisé avec CREATE_NEW ou UPDATE, le nom du formulaire référencé doit respecter la convention d'affectation de noms zdetailxxx_sous-objet.htmpl, xxx représentant les caractères, et *sous-objet* le nom du sous-objet.	CREATE_NEW DISPLAY_FORM JUST_GRONK_IT MENU SEARCH SET_MENU SHOW_DETAIL UPDATE

Variables	description	Service Opérations
KEEP.*nom*	Spécifie la valeur pouvant être enregistrée et transmise entre des pages.	CREATE_NEW GENERIC_LIST SEARCH UPDATE
KEY.*nom_attr*	Similaire à la variable SET.*nom_attr*, à la différence près qu'elle spécifie une recherche sur *nom_attr*, qui doit désigner une autre table ou un autre objet.	UPDATE
NEXT_PERSID	Spécifie l'ID persistant du prochain enregistrement à afficher.	UPDATE
PERSID	Spécifie l'ID persistant d'un enregistrement à afficher. Vous pouvez spécifier cette variable de l'une des manières suivantes : Directement, avec un ID persistant composé d'un nom de sous-objet, du signe deux points (:) et d'un ID de base de données unique sous la forme d'un nombre entier. Par exemple, PERSID=chg:1234 spécifie la demande de changement avec l'ID de base de données 1234. Indirectement, avec un ID persistant composé d'un nom de sous-objet, du signe deux-points (:), d'un nom d'attribut, d'un second signe deux-points (:) et d'une valeur. Cette forme de PERSID spécifie l'enregistrement du sous-objet spécifié dont l'attribut a la valeur définie. Par exemple, PERSID=chg:chg_ref_num:demo:3 spécifie la demande de changement dont le numéro de référence est demo:3.	SHOW_DETAIL UPDATE
PRESET PRESET_REL	Spécifie les valeurs d'un ou plusieurs attributs de l'enregistrement créé suite à l'utilisation de la variable CREATE_NEW. Si la variable CREATE_NEW n'est pas spécifiée, la variable PRESET est ignorée.	CREATE_NEW

Variables	description	Service Opérations
QBE.*op*.*nom_attr*	Spécifie les valeurs à utiliser lors d'une recherche. Ces valeurs sont identifiées à l'aide d'un mot clé QBE, *nom_attr* correspondant à un nom d'attribut définissable d'un ticket et *op* indiquant de rechercher si l'attribut : EQ est égal à la valeur NE est différent de la valeur GT est supérieur à la valeur LT est inférieur à la valeur GE est supérieur ou égal à la valeur LE est inférieur ou égal à la valeur NU correspond à null NN ne correspond pas à null IN correspond à l'expression SQL LIKE KY contient le texte entré Si vous ne définissez aucune variable QBE, c'est la fenêtre de recherche standard qui s'affiche.	SEARCH
SET.*nom_attr*	Spécifie le nom de l'attribut à utiliser lors de la création d'un ticket, *nom_attr* correspondant à un attribut définissable dans un ticket. Les noms d'attributs varient en fonction de l'objet sous-jacent. Tous les objets et leurs attributs se trouvent dans les fichiers *.maj du répertoire majic dans bopcfg, comme indiqué dans le Manuel de référence technique de CA SDM.	CREATE_NEW UPDATE
SET.*id*	Spécifie l'ID de la base de données de la ligne à mettre à jour.	UPDATE
SKIPLIST	Si cette variable est définie à 1, la liste des résultats de la recherche ne s'affiche pas lorsqu'un seul résultat est renvoyé, mais le détail correspondant en lecture seule s'affiche directement.	SEARCH
use_template	Si cette variable est définie à 1, l'opération SEARCH renvoie une liste de modèles. Le modèle renvoyé sélectionné sera utilisé dans l'opération CREATE_NEW pour renseigner un nouvel enregistrement. Cette variable est valide pour les demandes de changement, les demandes client et les demandes.	CREATE_NEW SEARCH

Informations complémentaires :

Syntaxe des variables PRESET, PRESET_REL, ALG_PRESET et ALG_PRESET_REL (page 467)

Syntaxe des variables PRESET, PRESET_REL, ALG_PRESET et ALG_PRESET_REL

Les mots clés PRESET, PRESET_REL, ALG_PRESET et ALG_PRESET_REL dans l'adresse URL spécifient les valeurs initiales respectivement pour les attributs du ticket et son journal d'activité. Il existe deux formats :

[ALG_]PRESET=*attr*:*valeur*

Indique que l'attribut spécifié du ticket ou du journal d'activité doit être défini à la valeur spécifiée. Par exemple, la spécification suivante définit la description du nouveau ticket à « Bonjour ».

```
PRESET=description:Bonjour
```

[ALG_]PRESET_REL=attr:obj.attr-rel:attr-test:valeur

Indique que l'attribut spécifié du ticket ou du journal d'activité doit être défini à une valeur copiée d'une autre table de base de données. La valeur est copiée de l'attribut *attr-rel* de l'*objet* dont le paramètre *attr-test* a la *valeur* spécifiée. Par exemple, la spécification suivante définit l'attribut analyste du nouveau ticket à l'ID du contact dont l'ID d'utilisateur est xyz123 :

PRESET_REL=analyst:cnt.id:userid:xyz123

Lorsque ce format est utilisé, la requête doit extraire un seul enregistrement. Si plusieurs contacts (ou aucun) ont l'ID d'utilisateur xyz123, l'exemple de spécification PRESET est sans effet.

Les mots clés PRESET, PRESET_REL, ALG_PRESET et ALG_PRESET_REL peuvent figurer autant de fois que vous le souhaitez dans une adresse URL, ce qui permet de définir plusieurs attributs. Autrement, un opérande à un seul mot clé peut spécifier plusieurs valeurs séparées par les signes @@. Si vous utilisez le séparateur "@@", vous ne pouvez pas mélanger les formats de valeur pour les mots clés [ALG_]PRESET et [ALG_]PRESET_REL. L'exemple suivant présente deux manières de spécifier des valeurs pour la description du ticket, le résumé et l'analyste :

```
PRESET=description:Bonjour+PRESET=summary:Bonjour à
tous+PRESET_REL=analyst:cnt.id:userid:xyz123
PRESET=description:Bonjour@@summary:Bonjour à
tous+PRESET_REL=analyst:cnt.id:userid:xyz123
```

Pour les demandes, les demandes client, les incidents, les problèmes et les demandes de changement, PRESET et PRESET_REL gèrent un attribut de mot clé ASSET permettant de lier un objet à un actif. L'attribut ASSET met à jour l'attribut affected_resource d'une demande, d'un incident ou d'un problème, ou l'actif LREL d'une demande client ou d'une demande de changement.

Exemples de liens

Les exemples de lien suivants n'incluent pas le chemin d'accès à CA SDM. Toutes les URL de CA SDM commencent avec un codage sous la forme suivante :

http://*nom_hôte*[:*port*]/CAisd/pdmweb.exe

Dans cet exemple, *nom_hôte* est le nom de votre serveur, et *port* (facultatif) est le numéro de port si vous utilisez Tomcat. Ce codage est représenté par des points de suspension (...) dans les exemples d'adresses URL suivants :

- Pour créer une demande avec un utilisateur concerné avec l'ID d'utilisateur tooda01, utilisez l'exemple d'URL suivant :

  `…?OP=CREATE_NEW+FACTORY=cr+PRESET_REL=customer:cnt.id:userid:tooda01`

- Pour afficher la liste de toutes les demandes affectées à l'ID d'utilisateur tooda01, utilisez l'exemple d'URL suivant :

  `…?OP=SEARCH+FACTORY=cr+QBE.EQ.assignee.userid=tooda01`

- Pour afficher le formulaire détaillé pour la demande 1234, utilisez les exemples d'URL suivants :

  `…?OP=SHOW_DETAIL+FACTORY=cr+PERSID=cr:ref_num:1234 (vue en mode lecture seule)`

  `…?OP=UPDATE+FACTORY=cr+PERSID=cr:ref_num:1234 (vue en mode mise à jour)`

Remarque : Il est possible d'ignorer le protocole de contrôle de connexion en utilisant les services Web pour l'authentification. Pour plus d'informations sur la méthode getBopsid(), reportez-vous au Manuel de référence technique de CA SDM.

Personnalisation avancée

Vous devez être connaître divers aspects liés à la personnalisation des pages Web si vous choisissez d'utiliser d'autres outils que l'Outil de conception Web pour modifier HTMPL ou si vous avez des exigences de personnalisation inhabituellement complexes. Cependant, nous vous recommandons vivement de travailler avec l'outil WSP pour personnaliser les pages Web de CA SDM avant d'essayer une autre approche. L'outil WSP peut effectuer pratiquement toutes les personnalisations nécessaires et gère automatiquement les demandes client standard, telles que le placement des mises à jour dans le répertoire site mods et la distribution des fichiers publiés à tous les serveurs.

Moteur Web et mémoire cache

Pour personnaliser des pages Web, il est utile de comprendre la structure du serveur Web CA SDM. L'interface Web utilise soit un conteneur de servlet J2EE tel que Tomcat, soit un serveur HTTP standard tel qu'Apache ou IIS (Microsoft Internet Information Server). Lorsqu'un utilisateur appelle une page Web d' CA SDM, le serveur HTTP appelle le programme Web fourni, pdmweb.exe.

Au démarrage, le programme pdmweb.exe établit une connexion à un démon CA SDM (ou à un service Windows) appelé moteur Web. Le moteur Web interprète l'appel de l'utilisateur. Pour la plupart des requêtes, le moteur Web doit rechercher un fichier modèle (HTMPL) et le convertir en HTML standard. Généralement, pour effectuer la conversion, le moteur Web doit communiquer avec un serveur CA SDM pour lire ou mettre à jour la base de données et inclure des informations de base de données dans le HTML généré. Une fois le HTML prêt, le moteur Web l'envoie au programme pdmweb.exe qui le renvoie au navigateur de l'utilisateur.

Afin d'optimiser les performances, le moteur Web ne lit normalement qu'une fois chaque fichier HTMPL. Après avoir analysé le fichier et déterminé la manière de le convertir en HTML, le moteur Web conserve le fichier analysé dans sa mémoire cache, ce qui réduit sensiblement le temps de traitement la prochaine fois que le fichier sera demandé. Si la mémoire cache est très bénéfique dans un environnement de production, ce n'est pas toujours le cas dans un environnement de développement, dans la mesure où il est nécessaire de recycler le moteur Web ou d'exécuter l'utilitaire pdm_webcache pour que les modifications des fichiers HTMPL prennent effet. Dans un environnement de développement, vous pouvez contourner cette exigence en définissant la propriété du fichier de configuration SuppressHtmplCache. Pourtant, nous vous recommandons de ne pas supprimer le cache HTMPL dans un environnement de production en raison de l'impact important qu'a cette opération sur le moteur Web.

Remarque : Pour plus d'informations, reportez-vous au *Manuel d'administration.*

Les pages Web publiées par le programme pdmweb.exe sont générées par la lecture des fichiers HTMPL dont l'utilisation génère les fichiers HTML. Les fichiers de modèle HTML sont identifiés par le suffixe .htmpl. Vous pouvez modifier ces fichiers modèles et personnaliser ainsi les pages Web de CA SDM.

Utilitaire pdm_webcache

L'utilitaire pdm_webcache permet de supprimer un ou plusieurs formulaires HTMPL de la mémoire cache du moteur Web. Le moteur Web doit alors aller chercher ces formulaires sur le disque lors de leur utilisation suivante, et les modifications apportése aux formulaires sont appliquées.

`pdm_webcache [-f nom-formulaire] [-g groupe-formulaires] [-i interface] [-p processus] [-v]`

-f *nom-formulaire*

Spécifie le nom du groupe de formulaires à supprimer de la mémoire cache (detail_cr.htmpl, par exemple). Vous pouvez utiliser le signe "%" (ou "*") comme caractère générique pour sélectionner plusieurs formulaires. Par exemple, la spécification :

-f detail%

sélectionne tous les formulaires détaillés.

Cet argument est facultatif. S'il n'est pas défini, tous les formulaires présents dans la mémoire cache sont sélectionnés.

-g *groupe-formulaires*

Spécifie le nom du groupe de formulaires à supprimer de la mémoire cache (Analyste, par exemple). Vous pouvez utiliser le signe "%" (ou "*") comme caractère générique pour sélectionner plusieurs groupes de formulaires**.** Par exemple, la spécification :

-g Ana%

sélectionne tous les groupes de formulaires commençant par "Ana".

Cet argument est facultatif. S'il n'est pas défini, tous les groupes de formulaires présents dans la mémoire cache sont sélectionnés.

-i *interface*

Spécifie le nom de l'interface Web à supprimer de la mémoire cache, tel qu'analyste, client ou employé. Vous pouvez utiliser le signe « % » (ou « * ») comme caractère générique. Par exemple, la spécification :

-i a%

sélectionne l'interface Web analyste.

Cet argument est facultatif. S'il n'est pas défini, toutes les interfaces du cache sont sélectionnées.

-p *processus*

Spécifie le nom du processus du moteur Web dont la mémoire cache doit être modifiée, par exemple web:local.

Cet argument est facultatif. S'il n'est pas défini, tous les moteurs Web sont sélectionnés.

-v

Spécifie le mode de sortie prolixe. Lorsque cet argument est défini, pdm_webcache indique le nom complet de chaque formulaire supprimé de la mémoire cache sous la forme suivante :

interface:*groupe-formulaires*:*nom-formulaire*

Cet argument est facultatif. S'il n'est pas défini, pdm_webcache indique uniquement le nombre de formulaires supprimés de la mémoire cache de chaque moteur Web.

Modification des modèles HTML

Généralement, vous pouvez effectuer deux types de modifications :

- Vous pouvez effectuer des modifications qui seront visibles par l'utilisateur mais qui ne seront pas altérées par l'interface Web avant d'être affichées. Par exemple, vous pouvez ajouter le fichier GIF du logo de votre entreprise aux pages de l'interface Web en insérant la référence au modèle approprié ou ajouter un code JavaScript à votre page pour valider les données entrées. Les modifications apportées au fichier HTMPL qui ne sont pas contenues dans une balise PDM, telle que définie ci-dessous, sont transmises inchangées dans le code HTML qui est renvoyé à l'utilisateur.
- Vous pouvez modifier les sections des modèles pouvant être remplacées. Par exemple, vous pouvez ajouter des données d'application à la page de détail de la demande.

Plusieurs types d'entrées de modèle vous permettent d'effectuer les opérations suivantes :

- afficher des informations provenant de CA SDM pour l'utilisateur ;
- définir une page de requête ;
- créer des liens vers d'autres pages de CA SDM à l'aide de balises de liens.

Fichiers à ne pas modifier

Certains modèles HTMPL et fichiers JavaScript contiennent des informations nécessaires à de nombreux formulaires Web de CA SDM. Ces informations dépendent de la version et sont essentielles au bon fonctionnement de l'interface Web de CA SDM. C'est pourquoi ces fichiers sont toujours remplacés lors de la publication d'une nouvelle version de CA SDM ; les modifications apportées ne sont pas migrées.

Les modèles concernés par cette restriction sont les suivants :

ahdtop.htmpl

Contient des styles, des scripts et des variables JavaScript utilisés dans toute l'interface Web de CA SDM. Ce fichier fait partie du frameset principal de l'interface Web. Il est toujours présent en cours de session. Tous les formulaires CA SDM ont accès à la variable JavaScript ahdtop qui fait référence à la fenêtre contenant ahdtop.htmpl.

menu_frames.htmpl

Définit le frameset HTML utilisé par le formulaire principal de CA SDM.

msg_cat.js

Contient le texte de tous les messages utilisés dans les fichiers JavaScript de CA SDM.

reports.htmpl

Contient les données requises pour les rapports Web.

std_body.htmpl

Contient les informations standard utilisées au début de la section BODY de la plupart des modèles HTMPL.

std_footer.htmpl

Contient les informations standard utilisées à la fin de la section BODY de la plupart des modèles HTMPL.

std_head.htmpl

Contient les informations standard utilisées au début de la section HEAD de presque tous modèles HTMPL.

styles.htmpl

Contient les styles CSS utilisés dans toute l'interface Web de CA SDM.

Si vous ne pouvez pas modifier ces fichiers directement, vous pouvez leur ajouter des informations. A chaque fichier restreint xxx.htmpl (à l'exception de menu_frames.htmpl et reports.htmpl) correspond un fichier xxx_site.htmpl que vous pouvez personnaliser. Par exemple, vous pouvez ajouter des informations supplémentaires à ahdtop.htmpl en personnalisant ahdtop_site.htmpl ou ajouter de nouveaux messages en personnalisant msg_cat_site.js.

Le fichier xxx_site.htmpl correspondant à chaque fichier restreint est chargé après le fichier principal ; vous pouvez donc remplacer ou modifier JavaScript dans le fichier principal. Soyez prudent lorsque vous ajoutez des informations, car toute modification maladroite dans ces fichiers risque d'entraîner des problèmes inattendus dans l'ensemble de l'interface Web de CA SDM.

Informations complémentaires :

Répertoires utilisés par le serveur HTTP (page 476)

Recommandations pour les nouveaux fichiers HTMPL

Vous pouvez ajouter vos propres fichiers HTMPL à l'interface Web de CA SDM. Suivez les recommandations suivantes pour vous assurer que votre fichier HTMPL fonctionne correctement avec le reste de l'interface de CA SDM :

1. Insérez l'instruction suivante dans la section <HEAD> du fichier. Elle doit suivre l'instruction <TITLE> (si elle existe). Elle définit plusieurs variables globales JavaScript requises par l'interface Web de CA SDM et enregistre votre page dans le gestionnaire de fenêtres de CA SDM :

   ```
   <PDM_INCLUDE FILE=std_head.htmpl>
   ```

2. Insérez l'attribut suivant dans la balise <BODY> du fichier. Il permet au gestionnaire de fenêtres de CA SDM d'effectuer le suivi de votre page :

   ```
   onUnload="deregister_window()"
   ```

3. Insérez l'instruction suivante au début de la section <BODY> de votre fichier. L'argument "menubar=no" est facultatif ; s'il est défini, il supprime la barre de menus de CA SDM :

   ```
   <PDM_INCLUDE FILE=std_body.htmpl [menubar=no]>
   ```

4. Insérez l'instruction suivante à la fin de la section <BODY> de votre fichier.

   ```
   <PDM_INCLUDE FILE=std_footer.htmpl>
   ```

Ajout d'informations d'état définies par l'utilisateur

De nombreux clients souhaitent pouvoir insérer leurs propres informations d'état dans les pages Web de CA SDM pour qu'CA SDM les transmette à toutes les pages suivantes utilisées par la session de l'utilisateur. Ces informations sont accessibles à l'aide d'instructions conditionnelles insérées dans les fichiers HTMPL.

Vous obtenez les informations d'état d'une session utilisateur en définissant l'attribut spécial USER_STATE dans vos liens ou dans vos formulaires. Une fois la soumission au moteur Web de CA SDM effectuée, chaque page présentée à l'utilisateur contient la variable HTMPL USER_STATE disponible et définie à sa dernière valeur.

Voici quelques exemples de définition d'une entrée dans CA SDM à partir d'un autre endroit de votre site, par exemple à partir des pages destinées à votre équipe commerciale :

- Utilisation d'un lien hypertexte

  ```
  <a href="/CAisd/pdmweb.exe?USER_STATE=Ventes">Centre de services</a>
  ```

- Utilisation d’un formulaire comportant un champ caché

  ```
  <form action="http://votre_hôte.com/CAisd/pdmweb.exe">
  <input type=hidden name=USER_STATE value=Ventes>
  ```

  Cliquez sur le bouton pour accéder au Centre de services.

  ```
  <input type=submit>
  </form>
  ```

Vous pouvez ensuite personnaliser vos formulaires HTMPL en fonction des informations d'état :

```
<PDM_IF "$USER_STATE" == "Ventes">
```

informations personnalisées pour l’équipe commerciale

```
<PDM_ELIF "$USER_STATE" == "Ingénierie">
```

informations personnalisées pour les ingénieurs

```
<PDM_ELSE>
```

informations pour les autres personnes

```
</PDM_IF>
```

Création directe d'une demande à partir d'un modèle

Il est possible de créer une demande directement à partir d'un modèle à l'aide d'une URL.

Exemple :

```
http://nom_machine/CAisd/pdmweb.exe?FACTORY=cr+OP=CREATE
NEW+PERSID=cr:3106+use_template=1
```

où cr:3106 est l’ID persistant du modèle.

Configuration d'un billet à clôture rapide avec des options prédéfinies

Dans la vue Profil Rapide, vous pouvez créer un billet à clôture rapide, par exemple un incident à clôture rapide. Ajoutez une chaîne prédéfinie à l'URL lorsque vous créez un billet à clôture rapide pour ajouter automatiquement une description, un résumé ou d'autres informations de champ.

Pour ajouter une chaîne prédéfinie à la fonction de billet à clôture rapide, effectuez les opérations suivantes :

1. Copiez le fichier ahdtop_site.htmpl de NX_ROOT/bopcfg/www/htmpl/default vers NX_ROOT/site/mods/htmpl/www/default.
2. Modifiez le fichier ahdtop_site.htmpl file (page 475) à l'aide de la variable appropriée (en fonction du type de billet à clôture rapide).
3. Connectez-vous à CA SDM.
4. Créez un billet à clôture rapide.

   Les renseignements prédéfinis sont ajoutés au billet.

Créer un ticket à clôture rapide avec des options prédéfinies

Vous pouvez créer un ticket à clôture rapide, par exemple un incident à clôture rapide, dans le profil rapide. L'option Clôture rapide vous permet d'ouvrir et de fermer un nouveau ticket en une opération, par exemple lorsque vous ouvrez et résolvez l'incident dans la même session. Vous pouvez ajouter une chaîne prédéfinie à l'URL lorsque vous créez un ticket de clôture rapide pour ajouter automatiquement une description, un résumé ou d'autres informations de champ.

Pour créer un ticket à clôture rapide avec des options prédéfinies

1. Copiez le fichier ahdtop_site.htmpl de NX_ROOT/bopcfg/www/htmpl/default vers NX_ROOT/site/mods/htmpl/www/default.
2. Modifiez le fichier ahdtop_site.htmpl pour ajouter la variable appropriée (selon le type de ticket à clôture rapide) avec la chaîne prédéfinie.
   - Quick Close Incident—var quick_close_preset_in
   - Quick Close Problem—var quick_close_preset_pr
   - Quick Close Request—var quick_close_preset_cr
   - Quick Close Issue—var quick_close_preset_iss

   La chaîne suivante, par exemple, définit la description sur HelloIncident et le résumé sur HelloIncidentSummary pour un incident à clôture rapide.

   ```
   var quick_close_preset_in =
   "PRESET=description:HelloIncident@@summary:HelloIncidentSummary";
   ```

3. Connectez-vous à CA SDM.
4. Sélectionnez Afficher, Profil rapide sous l'onglet Centre de services.

   La fenêtre Recherche de contacts disposant de profils rapides s'ouvre.
5. Remplissez un ou plusieurs champs de recherche pour le contact, puis cliquez sur Rechercher.

   La Liste de contacts disposant de profils rapides répertorie les contacts correspondant à vos critères de recherche.
6. Sélectionnez un contact.

   Le volet de droite affiche les informations de ce contact.
7. Cliquez sur Clôture rapide.

   Le ticket est créé avec les informations prédéfinies.

Répertoires utilisés par le serveur HTTP

L'installation par défaut de CA SDM définit deux répertoires virtuels pour votre serveur HTTP :

- Le répertoire virtuel CAisd pointe vers le répertoire suivant dans l'installation de CA SDM :

  Sous Windows : *répertoire-installation*\bopcfg\www\wwwroot

  Sous UNIX : $NX_ROOT/bopcfg/www/wwwroot
- Le répertoire virtuel CAisd/sitemods pointe vers le répertoire suivant dans l'installation d'CA SDM :

  Sous Windows : *répertoire-installation*\site\mods\www\wwwroot

  Sous UNIX : $NX_ROOT/site/mods/www/wwwroot

Les sous-répertoires de ces répertoires virtuels sont les suivants :

Sous-répertoire	Contenu
css	Feuilles de style
help	Aide de l'interface Web
html	Fichiers HTML
img	Fichiers graphiques
scripts	JavaScript
sitemods	Personnalisations définies par le site

Si vous décidez de personnaliser l'un des fichiers des répertoires css, html, img ou scripts, il est fortement déconseillé d'en modifier la version originale dans /CAisd. Copiez plutôt le fichier dans le sous-répertoire approprié de /CAisd/sitemods. Par exemple, pour modifier une feuille de style de /CAisd/css, enregistrez votre version personnalisée dans /CAisd/sitemods/css. Lorsque le moteur Web analyse un fichier HTMPL, il modifie automatiquement les noms de fichiers commençant par $CAisd pour désigner sitemods si le fichier existe dans un sous-répertoire de sitemods.

L'utilisation du répertoire /CAisd/sitemods présente les avantages suivants :

- Vous conservez un enregistrement des fichiers distribués que vous avez modifiés.
- Vous pouvez accéder facilement à la version originale en cas de question ou de problème.
- L'installation d'une mise à niveau ou d'une nouvelle version est plus facile, car CA SDM ne place rien dans le répertoire /CAisd/sitemods.

Remarque : Il n'existe pas de sous-répertoire /CAisd/sitemods/help. Les données de l'aide se trouvant dans des fichiers HTML standard (et non dans des modèles HTMPL), le moteur Web ne peut pas modifier dynamiquement les références de fichier. Pour personnaliser l'aide, introduisez vos modifications dans /CAisd/help.

Le sous-répertoire HTML contient quelques fichiers très utilisés qui ne nécessitent pas de traitement du moteur Web et qui peuvent améliorer les performances lorsqu'ils sont placés dans la mémoire cache du navigateur. Si vous créez une version personnalisée de l'un de ces fichiers, vérifiez soigneusement les références de ce fichier à d'autres fichiers personnalisés. Etant donné qu'il n'y a pas de traitement du moteur Web, vous devez insérer manuellement une référence à sitemods si nécessaire.

Téléchargement des pièces jointes au format PDF

Quand vous téléchargez une pièce jointe au format PDF et que vous essayez de l'afficher dans CA SDM, le fichier PDF peut ne pas s'afficher correctement ou une fenêtre vide peut apparaître après une mise à niveau vers Adobe Acrobat 7.0 ou 8.0. Avec CA SDM, vous pouvez afficher le fichier PDF correctement en effectuant la procédure suivante :

1. Définissez le paramètre *forceDecompressOnDownload* sur YES dans $NX_ROOT\bopcfg\www\CATALINA_BASE\webapps\CAisd\WEB-INF\web.xml.

   Remarque : Sous Linux, $NX_ROOT est /opt/CAisd.

2. Redémarrez les services CA SDM.

Recherche d’informations dans les tables de références

Les champs de saisie d'un formulaire détaillé modifiant un enregistrement de base de données sont nommés SET.nom_attr. Quand l'enregistrement est enregistré, les données des champs SET sont copiées directement dans l'enregistrement sous-jacent. Dès lors, un champ d’entrée d’un attribut faisant référence à une autre table doit contenir le REL_ATTR (clé étrangère) de cette table. Il s’agit normalement de l’ID (id), de l’ID persistant (persistent_id) ou du code de l’enregistrement de référence.

Les utilisateurs ne fournissent pas directement les valeurs REL_ATTR, et les champs SET des attributs faisant référence à une autre table sont masqués. Le champ visible dans le formulaire est nommé KEY.*nom_attr* et contient le nom commun de l'enregistrement référencé. Un nom commun doit être converti en REL_ATTR pour mettre à jour l’enregistrement. Cette opération peut être réalisée dans plusieurs cas :

- Pour les champs permettant d'opérer une sélection dans une liste déroulante, la valeur SET est fournie directement par la liste déroulante.
- Pour les champs offrant une fonction de recherche lorsque l'utilisateur clique sur la recherche et sélectionne un élément, la valeur SET est copiée à partir de l'élément sélectionné.
- Pour les champs offrant une fonction de recherche où l'utilisateur entre une clé partielle identifiant l'enregistrement de façon univoque puis clique sur l'étiquette, le navigateur demande la valeur SET au serveur et la copie, ainsi que la clé complète, dans le formulaire.
- Si la propriété Autofill du fichier de configuration est fournie ou utilisée par défaut et que l'utilisateur fournit une clé partielle identifiant l'enregistrement de façon univoque et clique sur Carnet pour quitter le champ, le navigateur demande la valeur SET au serveur et la copie, ainsi que la clé complète, dans le formulaire.

Sinon, quand l'enregistrement est sauvegardé avec une valeur KEY mais sans valeur SET, le moteur Web résout la valeur durant la sauvegarde. Si une valeur KEY ne peut pas être résolue en une valeur SET unique, la sauvegarde est bloquée, et le formulaire de modification s'affiche de nouveau.

Si un formulaire s'affiche de nouveau suite à un échec de la sauvegarde résultant d'un échec de la résolution de la recherche, les variables suivantes sont disponibles dans le fichier HTMPL pour chaque champ d'attribut sur lequel une recherche a été effectuée :

LIST_*attr*

Contient toutes les correspondances trouvées. Il s’agit généralement de la partie droite du champ SOURCE= dans une instruction <PDM_SELECT>.

FLAGS_*attr*

Définie à l'une des valeurs suivantes :

0

Affiche le champ de recherche initial.

1

Plus d'une et moins de MaxSelectList correspondances ont été trouvées (une liste <PDM_SELECT> s'affiche généralement dans ce cas).

2

Aucune correspondance trouvée.

3

Trop de correspondances ont été trouvées (plus de MaxSelectList).

SEARCH_STATUS_*chaîne attr*

Contient la chaîne de texte TooManyMatches du fichier web.cfg.

Remarque : Pour plus d'informations sur le fichier web.cfg, reportez-vous au *Manuel d'administration*.

Spécification des recherches sur les contacts

Lorsque vous spécifiez un contact (nom, prénom et deuxième prénom) dans un formulaire modifiable, vous pouvez en délimiter le nom avec des virgules (,) ou des espaces, mais pas les deux. Il est recommandé d'utiliser des virgules, car les noms comportent souvent des espaces imbriqués, ce qui peut poser des problèmes.

La combinaison de virgules et d'espaces n'étant pas autorisée, la présence de virgules implique que toutes les parties du nom sont séparées par une virgule ; s'il n'y a pas de virgule, les noms sont délimités par des espaces.

Les informations étant transmises à une requête SQL, le symbole de pourcentage (%) sert de caractère générique (joker). Par exemple, « P%, J% » correspond à « Public, Joseph », « Pont, Jeannette » et à tous les autres contacts dont le nom commence par P et le prénom par J. (La distinction entre majuscules et minuscules dépend de la base de données sous-jacente). De même, « P%, J% » renverrait les mêmes noms.

Cependant "P%, Jo D" ne renverrait pas tous les contacts dont le prénom est Jo, l'initiale du second prénom est D et le nom commence par P, puisque la présence d'une virgule signifie que tous les délimiteurs sont des virgules. Ainsi, le nom recherché serait "P%" et le prénom "Jo D". Pour éviter une telle erreur, spécifiez plutôt « P%, Jo, D ».

Prétraitement du moteur Web

Le moteur Web passe par deux phases lors du traitement d'un fichier HTMPL :

- La phase de prétraitement, pendant laquelle le fichier HTMPL et les fichiers référencés sont lus (notamment les fichiers référencés par les balises PDM_INCLUDE et PDM_MACRO). La sortie du prétraitement est une entrée dans la mémoire cache interne du moteur Web.
- La phase de génération, pendant laquelle le formulaire est lu à partir du cache et le fichier HTML est généré. La sortie de la génération est le fichier HTML fourni au navigateur.

La phase de prétraitement est généralement exécutée une fois pour chaque formulaire au cours de la durée de vie du moteur Web. La phase de génération a lieu chaque fois qu'un formulaire est demandé.

Vous pouvez utiliser les balises PDM_SET et PDM_EVAL durant la phase du préprocesseur pour générer et stocker des informations, telles que du texte HTML, que le moteur Web peut utiliser lors de la phase de génération.

Variables du préprocesseur

Les variables du préprocesseur commencent par la chaîne "$PRE.". Elles sont créées et actualisées avec la balise PDM_SET (page 451). Cette balise présente la syntaxe suivante lorsqu'elle est utilisée avec une variable de préprocesseur :

```
<PDM_SET PRE.nom[+]=valeur>
```

Cette balise affecte une variable de préprocesseur ou la met à jour, en la créant si nécessaire. Elle est traitée lorsque le moteur Web la rencontre pendant la lecture d'un formulaire. Seules les instructions PDM_IF de type invariant affectent la balise PDM_SET d'une variable de préprocesseur ; les autres instructions sont ignorées.

Détection des instructions PDM_IF de type invariant

Lors de l'analyse d'un formulaire, le moteur Web détecte les instructions PDM_IF de type invariant. Une instruction PDM_IF de type invariant est une instruction dont les arguments sont constitués exclusivement de littéraux, de variables d'environnement, de propriétés de constante et de variables de préprocesseur. Lorsque le moteur Web détecte une instruction PDM_IF de type invariant, il évalue sa condition immédiatement. Les effets sont les suivants :

- Les balises PDM_SET et PDM_EVAL qui sont ignorées par une instruction PDM_IF de type invariant sont ignorées. Toutes les autres balises pdm_eval et PDM_SET faisant référence à des variables de préprocesseur sont exécutées lors du traitement, même si elles sont contenues dans une instruction PDM_IF qui n'est pas de type invariant.

- Les références de variable de formulaire ignorées par une instruction PDM_IF de type invariant sont ignorées, et leur valeur n'est pas extraite lorsque le formulaire est utilisé. Vous pouvez utiliser cette technique pour améliorer la performance d'un formulaire. Par exemple, si un formulaire contient les valeurs suivantes, le moteur Web extrait la valeur de $args.def avant d'afficher le formulaire :

  ```
  <PDM_IF "$env.NX_OTB_MARKET == "itil" && "$args.a" == 1>
  <h1>Il s'agit du formulaire $args.def</h1>
  </PDM_IF>
  ```

  Pourtant, si le segment suivant a été écrit, le moteur Web détermine que la première instruction PDM_IF est de type invariant et extrait la valeur $args.def uniquement si $NX_OTB_MARKET est "itil".

  ```
  <PDM_IF "$env.NX_OTB_MARKET == "itil">
  <PDM_IF "$args.a" == 1>
  <h1>Il s'agit du formulaire $args.def</h1>
  </PDM_IF>
  </PDM_IF>
  ```

PDM_EVAL : Insérer du texte à partir d'une variable de préprocesseur

La balise PDM_EVAL insère la valeur d'une variable de préprocesseur dans l'entrée de l'analyseur du moteur Web. Si elle est utilisée dans une macro, son incidence est différée tant que la macro n'est pas terminée.

La balise PDM_EVAL fonctionne de la même manière que la balise PDM_INCLUDE ou PDM_MACRO. Elle insère le texte dans l'analyseur à l'emplacement de la balise, exactement comme si la valeur de sa variable avait été codée à la place de la balise.

La balise PDM_EVAL présente la syntaxe suivante :

```
<PDM_EVAL TEXT=PRE.nom>
```

où PRE.nom spécifie le nom de la variable de préprocesseur dont la valeur doit être insérée dans l'entrée du moteur Web

L'exécution de la balise PDM_EVAL peut être contrôlée par des instructions PDM_IF de type invariant.

Important : Sous UNIX, le LIBPATH doit être défini avant d'exécuter l'utilitaire. Utilisez pdm_task pour effectuer cette tâche. Par exemple, avant d'exécuter l'utilitaire, entrez "pdm_task pdm_eval".

Personnalisation sous forme de texte libre des formulaires détaillés

Les rubriques dans cette section décrivent la méthode de personnalisation au format libre de formulaires détaillé.

Utilisation de JavaScript dans les formulaires détaillés

Utilisez l'outil WSP pour ajouter vos champs à un formulaire détaillé ou pour réorganiser ou modifier les caractéristiques des champs inclus dans le formulaire par défaut. Cependant, la personnalisation d'un formulaire ne se limite pas toujours au simple ajout de nouveaux champs dans une grille. Plusieurs fonctions JavaScript sont intégrées dans CA SDM pour vous aider à fusionner vos propres personnalisations dans un formulaire détaillé combiné et à donner à celui-ci l'apparence souhaitée. Ces fonctions sont résumées comme suit :

- Vous pouvez placer un élément HTML quelconque avant l'instruction DetailForm() ou après l'instruction endDetail() sans affecter le fonctionnement du formulaire détaillé.
- Vous pouvez utiliser la fonction detailEndTable() pour fermer le tableau qui met en page les éléments du formulaire détaillé dans une grille. Cela fait, vous pouvez mettre en page votre propre élément HTML au format désiré. Dans ce cas, l'élément HTML se trouve à l'intérieur du formulaire détaillé, et tous ses champs de formulaire sont soumis au moteur Web lorsque l'utilisateur clique sur Enregistrer. Vous pouvez utiliser la fonction detailNextID() pour générer pour vos éléments HTML des champs ID afin de les intégrer à la navigation sans souris dans le formulaire détaillé. Vous trouverez plusieurs exemples de cette technique dans les onglets de carnet tels que xx_alg_tab.htmpl.
- Vous pouvez faire suivre votre propre élément HTML d'une macro dtlStartRow pour redémarrer le formatage du formulaire détaillé standard. Cette macro lance une seconde grille dont les champs ne sont pas nécessairement alignés sur ceux de la première. Cette technique est utilisée dans chaque onglet de carnet.
- Pour insérer un élément personnalisé à la fin d'une ligne, vous pouvez utiliser la fonction detailWriteRow() pour écrire le contenu d'une ligne sans la fermer. Le code qui génère le bouton 24 heures dans detail_cr.htmpl et detail_iss.htmpl illustre cette technique.
- Pour spécifier explicitement le contenu d'un élément d'une ligne sans fermer le tableau qui met en page la grille, vous pouvez utiliser la fonction detailRowHdr() pour spécifier le texte de l'en-tête et la fonction detailSetRowData() pour spécifier celui des données. Le code qui génère le champ du minuteur dans les pages detail_cr.htmpl et detail_iss.htmpl illustre cette technique.
- Si vous disposez d'une fonction permettant de valider la valeur d'un champ (normalement dans un gestionnaire d'événement) et souhaitez que ses résultats soient signalés dans un rapport pendant une validation côté navigateur (de façon à ce qu'un champ erroné apparaisse avec une épaisse bordure rouge et qu'un message d'erreur s'affiche dans une bande jaune en haut du formulaire), utilisez la fonction detailReportValidation(). Cela est illustré dans la fonction validate_duration() utilisée pour valider les champs de durée dans xx_candp_tab.htmpl. La fonction validate_duration() se trouve dans le fichier val_type.js.

- Pour examiner le code HTML généré pour un formulaire détaillé, vous pouvez utiliser les fonctions docWrite() et docWriteln() au lieu des fonctions standard document.write() et document.writeln(). Ensuite, si vous invoquez la fonction holdHTMLText() dans la section <HEAD> du formulaire, CA SDM affiche un formulaire de débogage contenant une zone TEXTAREA dans laquelle apparaît tout le code HTML généré pour le formulaire, que vous pouvez alors examiner ou couper et coller dans un outil de validation.

Lorsque vous préparez vos modifications, n'oubliez pas que le formulaire détaillé combiné s'affiche dans les modes de lecture seule et de modification. Si les personnalisations s'appliquent spécifiquement à un mode ou à l'autre, vous pouvez tester le mode actif de deux manières :

- En JavaScript, l'expression _dtl.edit est vraie en mode de modification et fausse en mode de lecture seule.
- En JavaScript ou HTML ouvert, les instructions :

  ```
  <PDM_IF "$prop.nom_formulaire_3" == "edit">
  ```

  (Utilisé uniquement en mode édition)

  ```
  </PDM_IF>
  ```

  ou

  ```
  <PDM_IF "$prop.nom_formulaire_3" == "ro">
  ```

  (Utilisé uniquement en mode lecture seule)

  ```
  </PDM_IF>
  ```

  Utilisé pour mettre en évidence le code destiné uniquement aux modes édition ou lecture seule, respectivement.

detailEndTable()

Cette fonction ferme le tableau HTML qui met en page les éléments du formulaire détaillé dans une grille. Elle ne comporte aucun argument.

Vous pouvez démarrer une nouvelle grille à l'aide de la macro dtlStartRow(). Toutefois, les éléments de la nouvelle grille ne sont pas nécessairement alignés sur ceux de la grille précédente.

detailNextID([colspan,][lastelement])

Cette fonction renvoie une chaîne sous la forme :

" ID=df_*nn_nn* TABINDEX=*n* onFocus=*func* onBlur=*func*"

Si vous insérez cette chaîne dans un élément HTML, celui-ci applique les conventions de navigation sans souris de CA SDM, notamment l'accessibilité par les flèches et l'affichage en jaune pâle du champ dans lequel se trouve le curseur. La chaîne renvoyée commence par un espace et ne contient pas d'espace final.

colspan

Spécifie le nombre de colonnes de la grille utilisées par l'élément. Cet argument est facultatif. Sa valeur par défaut est un s'il n'est pas fourni. S'il n'est pas défini, l'élément est supposé recouvrir une colonne de la grille. Ceci affecte le comportement de la flèche. Vous pouvez omettre l'argument *colspan* même si l'argument *lastelement* est fourni.

lastelement

Valeur booléenne spécifiant si l'élément pour lequel l'ID est généré est le dernier de la ligne. Si elle n'est pas définie, l'élément est normalement suivi d'autres éléments. Ceci affecte le comportement de la flèche.

detailNextLinkID()

Cette fonction renvoie une chaîne sous la forme :

" ID=dflnk_*nn_nn* TABINDEX=0 onFocus=*func* onBlur=*func*"

Si vous insérez cette chaîne dans un élément HTML définissant un élément de lien, cet élément applique les conventions de navigation sans souris de CA SDM, notamment l'accessibilité par la flèche Haut et l'affichage en jaune pâle du champ dans lequel se trouve le curseur. La chaîne renvoyée commence par un espace et ne contient pas d'espace final.

Cette fonction n'accepte aucun argument.

detailReportValidation(field, has_error, emsg)

Cette fonction rapporte le résultat d'une validation de champ externe. En cas d'échec de la validation, le champ apparaît avec une épaisse bordure rouge, et le message d'erreur s'affiche dans une bande jaune en haut du formulaire. L'utilisateur n'est pas autorisé à sauvegarder l'enregistrement tant qu'une exécution subséquente de la fonction detailReportValidation() n'a pas signalé que le champ ne comporte pas d'erreur.

La fonction detailReportValidation() n'est utilisable que pour les champs enregistrés pour une validation côté navigateur. Tous les champs créés à l'aide de macros de formulaire détaillé sont automatiquement enregistrés pour une telle validation. Vous pouvez en enregistrer d'autres à l'aide de la fonction detailSetValidateFunction().

field

(Obligatoire) Spécifie l'objet élément de formulaire contenant le champ. La manière la plus simple de l'obtenir consiste à transmettre cet argument au gestionnaire d'événement effectuant la validation. Une autre méthode consiste à utiliser la fonction JavaScript standard document.getElementById().

has_error

(Obligatoire) Valeur booléenne ou nombre entier spécifiant si le champ est erroné. Le fait qu'un champ soit défini comme erroné empêche l'utilisateur de sauvegarder l'enregistrement, fait apparaître le champ avec une épaisse bordure rouge et affiche le message d'erreur fourni comme troisième argument dans une bande jaune en haut du formulaire. Le fait que le champ soit défini comme exempt d'erreur annule ces modifications.

emsg

Chaîne de texte spécifiant le message à afficher dans la bande jaune en haut du formulaire détaillé lorsque l'indicateur *has_error* est activé. Cet argument est obligatoire si l'indicateur *has_error* est activé.

detailSetValidate(hdrtext, is_required, maxsize)

Cette fonction spécifie que le dernier champ créé avec un ID fourni par la fonction detailNextID() fait l'objet d'une validation côté navigateur. La validation des champs obligatoires et des champs dotés d'une taille maximale s'opère automatiquement. Vous pouvez fournir d'autres formulaires de validation à l'aide des fonctions JavaScript ou des gestionnaires d'événement exécutant la fonction detailReportValidation().

N'invoquez la fonction detailSetValidate() que pour les champs de formulaire que vous avez définis et dont l'ID a été créé par detailNextID(). La fonction detailSetValidate() doit être invoquée immédiatement après la création du champ à valider. Il est superflu (au risque d'obtenir des résultats inattendus) d'invoquer la fonction detailSetValidate() pour des champs créés à l'aide des macros du formulaire détaillé.

hdrtext

(Obligatoire) Spécifie une chaîne utilisée pour identifier le champ dans les messages d'erreur.

is_required

(Obligatoire) Valeur booléenne ou nombre entier spécifiant si le champ est obligatoire. CA SDM vérifie automatiquement que tous les champs obligatoires sont renseignés chaque fois que l'utilisateur tente de sauvegarder un enregistrement.

maxsize

Nombre entier spécifiant la longueur maximale autorisée des données contenues dans le champ. CA SDM vérifie automatiquement que la longueur de tous les champs pour lesquels une valeur *maxsize* est spécifiée est inférieure à celle-ci chaque fois que l'utilisateur tente de sauvegarder un enregistrement. Cet argument est obligatoire. Pour supprimer la validation *maxsize*, spécifiez la valeur 0.

detailRowHdr(hdrtext, colspan, is_required)

Cette fonction conserve le texte de l'élément en-tête (TH) d'un élément de la grille. Ce texte n'est pas réellement écrit dans le formulaire tant que la fonction detailWriteRow() ou la macro dtlStartRow n'est pas invoquée.

hdrtext

Spécifie le texte de l'élément en-tête. Cet argument est obligatoire.

colspan

Spécifie le nombre de colonnes de la grille utilisées par l'élément. Cet argument est facultatif. Sa valeur par défaut est un s'il n'est pas fourni. S'il n'est pas défini, l'élément est supposé recouvrir une colonne de la grille. Ceci affecte le comportement de la flèche. L'argument *colspan* doit être fourni si l'argument *is_required* est fourni.

is_required

Indique si *hdrtext* doit s'afficher dans le style correspondant à un champ obligatoire. L'argument peut être une valeur booléenne, un nombre ou une chaîne. Un nombre ou une chaîne est interprété comme faux si sa valeur est zéro, et comme vrai dans le cas contraire. Cet argument est facultatif ; s'il n'est pas défini, *hdrtext* a le style d'un champ facultatif.

detailSetRowData(text)

Cette fonction conserve le texte de l'élément en-tête (TD) d'un élément de la grille. Ce texte n'est pas réellement écrit dans le formulaire tant que la fonction detailWriteRow() ou la macro dtlStartRow n'est pas invoquée. L'unique argument est le texte HTML de l'élément à conserver.

detailWriteRow()

Cette fonction écrit le code HTML conservé pour la ligne en cours. Ceci crée deux lignes de table HTML, l'une pour les éléments en-tête (TH) et l'autre pour les éléments données (TD). La fonction écrit également la balise <td> qui commence un nouvel élément données. La balise TD est automatiquement fermée par la macro dtlStartRow, de sorte qu'il est superflu (et incorrect) d'insérer des balises <td> dans le texte HTML qui suit detailWriteRow(). Cette fonction ne comporte aucun argument.

Comprendre les formulaires de liste

La section suivante fournit des informations générales sur la composition des formulaires de liste CA SDM. Nous vous recommandons d'utiliser le mode Conception de Outil de conception Web pour modifier ces formulaires.

Les formulaires de liste CA SDM sont définis à l'aide des macros suivantes (appelées avec la balise PDM_MACRO) :

lsStart

Commence une liste.

lsCol

Définit une colonne d’une liste.

lsWrite

Insère du texte dans la partie pdm_list d'une liste

lsEnd

Termine une liste.

La forme générale d'une liste utilisant ces macros est la suivante :

```
<pdm_nom macro=lsStart>
<pdm_macro name=lsCol hdr=hdr1 attr=attr1>
<pdm_macro name=lsCol hdr=hdr1 attr=attr1>
<pdm_macro name=lsEnd>
```

Ce qui génère du texte similaire au suivant dans le code de sortie HTML :

```
var rs = new Resultset();       From lsStart
rs.startList(); From lsStart
rs.header("hdr1"); From lsCol
rs.setData("attr1","options"); From lsCol
rs.header("hdr2"); From lsCol
rs.setData("attr2","options"); From lsCol
<PDM_LIST SOURCE=list> From lsEnd
rs.data(attr1) From lsCol/lsEnd
rs.data(attr2) From lsCol/lsEnd
</PDM_LIST> From lsEnd
```

Remarque : Il existe deux sections distinctes dans la liste de sortie, à savoir la section de configuration avant la balise <PDM_LIST> et la liste réelle entre les balises <PDM_LIST> et </PDM_LIST>. La macro lsCol utilise les variables de préprocesseur et la balise <PDM_SET> pour générer des données dans les deux sections de la liste. L'intégralité de la section de liste de la liste est créée par une balise <PDM_EVAL> générée par la macro lsEnd.

Pour insérer votre propre code JavaScript dans la section de configuration de la liste, incluez-le simplement à l'emplacement requis. Utilisez la macro lsWrite pour insérer votre propre code dans la section de liste de la liste.

Macro lsWrite

La macro lsWrite spécifie le texte de la section de liste d'une liste (partie entre les balises <pdm_list> et </pdm_list>). Le texte spécifié pour l'argument de texte de cette macro est différé, et il n'est pas écrit dans le code HTML de sortie avant la macro lsEnd.

lsWrite [both=no|yes]

text="xxx"

les deux

Spécifie que l'opérande de texte doit être écrit immédiatement dans le code HTML de sortie et dans la mémoire tampon du texte différé. Ceci peut être utile pour générer du code JavaScript afin d'ignorer sous conditions les informations de liste et de configuration générées par une macro lsCol ultérieure. Facultatif ; la valeur par défaut est non (no).

text

Spécifie le texte généré par cette macro. Le texte spécifié est différé jusqu'à la macro lsEnd.

Il est souvent souhaitable d'inclure des balises et des références à des variables de formulaire dans le texte généré par une macro lsWrite. Pour empêcher qu'elles ne soient interprétées par le moteur Web durant l'analyse de la macro lsWrite, conformez-vous aux règles de syntaxe suivantes :

- Si la macro lsWrite génère une balise_pdm, omettez les délimiteurs « < » et « > » de la balise. Ainsi, pour insérer une instruction <pdm_else> dans la section de liste de la liste, utilisez le code suivant :

  ```
  <PDM_MACRO NAME=lsWrite text="pdm_else">
  ```

Le moteur Web insère automatiquement les signes « < » et « > » avant de produire le texte lorsqu'il détecte que les quatre premiers caractères sont « pdm_ » (ou « PDM_ »).

- Si la macro lsWrite génère une référence à une variable de formulaire, codez un caractère @ à la place du caractère $ qui désigne la variable. Par exemple, pour générer une référence à la variable de liste $list.persistent_id, utilisez le code suivant :

  ```
  <PDM_MACRO NAME=lsWrite text="@list.persistent_id">
  ```

  Le moteur Web convertit automatiquement les caractères "@" en "$" avant de produire le texte. Pour produire un signe @, faites-le précéder d'une barre oblique inverse.

Personnalisation de Modifier dans la liste

Plusieurs formulaires de liste, tels que la liste des demandes et celle des demandes client, comprennent un bouton Modifier dans la liste. Si ce bouton est disponible quand un ensemble de résultats est affiché, l'utilisateur peut cliquer dessus pour remplacer le filtre de recherche par un petit formulaire de modification. Le formulaire de modification permet à l'utilisateur de mettre à jour des enregistrements directement dans le formulaire de liste. L'utilisateur peut même mettre à jour tous les éléments sélectionnés dans la liste en plaçant les nouvelles données souhaitées dans le formulaire de modification puis en cliquant sur Tout modifier.

La modification des données de la liste implique qu'il n'y plus de communication avec le serveur tant que l'utilisateur ne clique par sur Enregistrer. Lorsque l'utilisateur clique sur Enregistrer, toutes les mises à jour (marquées en surbrillance jaune) sont envoyées au serveur qui applique toutes les modifications en une fois, renvoie un message d'état et actualise la liste.

Vous pouvez personnaliser cette fonction en contrôlant si le bouton Modifier dans la liste est disponible dans un formulaire de liste particulier, de même qu'en contrôlant les champs visibles du formulaire de modification qui s'affiche lorsque l'utilisateur clique sur Modifier dans la liste.

Pour placer un bouton Modifier dans la liste dans un formulaire de liste, incluez l'instruction suivante dans la section <HEAD> du formulaire :

```
<SCRIPT LANGUAGE="JavaScript" SRC=$CAisd/CAisd/list_edit.js></SCRIPT>
```

Le simple ajout de cette instruction place le bouton dans le formulaire. Toutefois, le bouton est désactivé à moins que des instructions JavaScript spécifiant le contenu du formulaire de modification y figurent également. Ces instructions doivent se trouver juste avant la spécification de l'ensemble des résultats, sous la forme suivante :

Instructions	commentaires
startListEdit(_search_filter);	Spécifier exactement comme indiqué
listEditStartRow();	Spécifier exactement comme indiqué
listEditField("attr"[, "hdr"]);	Spécifier zéro ou plus
listEditReadonly("attr[", "hdr"]);	Spécifier zéro ou plus
endListEdit();	Spécifier exactement comme indiqué

L'instruction endListEdit() doit être suivie de l'instruction ResultSet() qui commence l'ensemble des résultats. Vous spécifiez les champs dans le formulaire de modification et leur ordre dans le formulaire en codant une ou plusieurs instructions listEditReadonly() ou listEditField().

startListEdit(_search_filter);

Cette instruction commence le formulaire de modification de liste. Elle doit être codée précisément comme *startListEdit(_search_filter);*.

listEditStartRow();

Cette instruction commence une nouvelle ligne de champs sur le formulaire de modification de liste. Elle doit être codée précisément comme *listEditStartRow();*. Vous placez une instruction listEditStartRow() juste après l'instruction startListEdit(). Vous pouvez également inclure des instructions listEditStartRow() supplémentaires dans les instructions listEditField() et listEditReadonly() qui spécifient les champs dans le formulaire.

listEditField(attr_name[,hdr]);

Cette instruction spécifie un attribut à inclure dans le formulaire de modification de liste.

attr_name

Spécifie le nom de l'attribut à inclure dans le formulaire de modification (y compris les points, si nécessaire). Tous les attributs spécifiés pour un formulaire de modification de liste doivent également figurer dans l'ensemble des résultats. L'attribut *nom_attr* spécifié doit être identique à celui spécifié dans l'instruction rs.showData() ou rs.showDataWithLink() qui ajoute l'attribut à l'ensemble des résultats.

L'attribut s'affiche sur le formulaire de modification dans le même format que dans le filtre de recherche. S'il ne figure pas dans le filtre de recherche, il est modifié dans une zone de texte de 20 caractères.

nom_attr est un argument obligatoire.

hdr

Spécifie le texte de l'en-tête dans le champ du formulaire de modification. Cet argument est facultatif. Si vous le ne définissez pas, le texte de l'en-tête est renseigné à partir du filtre de recherche. Si vous ne définissez pas hdr et si l'attribut ne figure pas dans l'entrée de filtre de recherche pour attr_name, le texte de l'en-tête correspond par défaut au nom de l'attribut entouré de points d'interrogation.

listEditReadonly(attr_name[,hdr]);

Cette instruction spécifie un attribut non modifiable à inclure dans le formulaire de modification de liste. Ses arguments ont la même signification que ceux de listEditField().

endListEdit();

Cette instruction termine le formulaire de modification de liste. Elle doit être codée précisément comme *endListEdit();*.

Intégration à vos propres pages Web

Vous pouvez intégrer la fonctionnalité d'interface Web de CA SDM à vos pages Web pour présenter une interface transparente à vos utilisateurs.

Remarque : Le moteur Web, à savoir l'exécutable servant de passerelle entre le serveur Web et le serveur CA SDM, permet à un même utilisateur d'établir plusieurs connexions simultanées. Plusieurs trames peuvent avoir une connexion ouverte avec le processus du moteur Web de CA SDM.

Vous pouvez intégrer les interfaces Web selon l'une des trois méthodes suivantes :

- en créant des liens entre vos pages Web et la page Web appropriée de CA SDM sans passer par la page de menu de l'interface Web ;
- en ajoutant des formulaires HTML à vos pages Web pour collecter les entrées et exécuter directement les opérations prises en charge, sans afficher aucune des pages d'entrée de données Web d'CA SDM ;
- en créant des groupes de formulaires Web pour associer des formulaires Web HTML aux utilisateurs en fonction de leur type d'accès. Similaires aux groupes de formulaires utilisés par l'interface d'administration, les groupes de formulaires Web vous permettent de personnaliser vos pages HTML.

Renseignements supplémentaires :

Opérations de serveur prises en charge (page 459)

Liaison aux fonctions de CA SDM

Vous pouvez établir des liaisons directes avec les fonctions majeures d'CA SDM sans afficher la page principale. Vous le faites généralement en accédant à la fenêtre contextuelle de la nouvelle fenêtre contenant les informations sur CA SDM. Vous pouvez également remplacer votre page Web par celle de CA SDM.

Dans les deux cas, le produit affiche la page demandée telle que l'utilisateur la voit dans une session normale, mais sans la page principale ni le tableau d'affichage. Si vous êtes analyste, affichez la page principale et le tableau d'affichage en sélectionnant l'option Restaurer le tableau d'affichage dans le menu Fichier, laquelle n'est disponible que dans les pages auxquelles vous avez accédé sans passer par la page principale.

Pour créer un lien qui ne passe pas par la page principale, spécifiez une adresse URL de la forme suivante :

```
http://nom_hôte[:port]/CAisd/pdmweb.exe?OP=opération+var=value+…
```

Dans cet exemple, *nom_hôte* est l'ordinateur hôte du serveur Web, *port* est le numéro de port (généralement 8080) requis uniquement si vous utilisez Tomcat comme serveur http, *opération* est l'une des *opérations prises en charge* et var=value est l'une des variables autorisées avec l'opération.

Par exemple, vous pouvez spécifier un lien qui charge le formulaire de création d'une demande comme suit :

```
<A HREF=http://nom-hôte/CAisd/pdmweb.exe?OP=CREATE_NEW+FACTORY=cr>Définir
l'appel</A>
```

Informations complémentaires :

Exemples de liens (page 468)

Publication de formulaires sur CA SDM

Vous pouvez également accéder aux fonctions de CA SDM en ajoutant à vos pages Web des formulaires HTML faisant référence aux opérations prises en charge (page 459). Si le formulaire soumis contient suffisamment d'informations pour exécuter l'opération, par exemple une création de demande, celle-ci est effectuée sans qu'aucun formulaire de saisie supplémentaire n'apparaisse.

Lorsque vous ajoutez un formulaire HTML à votre page Web :

- L'opération ACTION du formulaire correspond à l'adresse URL de pdmweb.exe.
- METHOD a la valeur POST.
- Soit le nom du bouton SUBMIT correspond à l'une des opérations prises en charge, soit vous avez un champ masqué nommé OP dont la valeur est l'une des opérations prises en charge (page 459).

Par exemple, pour créer un formulaire HTML qui charge la page de création d'une demande, entrez le code suivant :

```
<FORM ACTION=/CAisdCAisd/pdmweb.exe METHOD=POST>
<INPUT type=HIDDEN NAME=FACTORY VALUE=iss>
.
.
.
<INPUT type=SUBMIT NAME=CREATE_NEW VALUE=" OK ">
</FORM>
```

JavaScript Customization

L'interface Web de CA SDM utilise intensivement JavaScript et inclut plusieurs fichiers JavaScript dans le répertoire /CAisd/scripts. Pour personnaliser l'un des fichiers de script, enregistrez la version modifiée dans /CAisd/sitemods/scripts, comme indiqué dans la section Répertoires utilisés par le serveur HTTP (page 476).

Pour des raisons de performances, les fichiers JavaScript figurant dans le répertoire /CAisd/scripts sont compressés, débarrassés des commentaires et espaces superflus. Cette compression peut rendre leur lecture plus difficile. Les versions non compressées de tous les fichiers JavaScript sont situées dans l'un des répertoires suivants :

- (UNIX) $NX_ROOT/sdk/scripts
- (Windows) $NX_ROOT/sdk/scripts

Si possible, évitez de créer des versions personnalisées de fichiers JavaScript entiers ; chacun de ces fichiers définit plusieurs fonctions alors que vous pouvez ne vouloir en modifier qu'une. Dans la plupart des cas, vous pouvez remplacer des fonctions individuelles en plaçant une version modifiée dans le fichier JavaScript sitemods.js. Nous vous recommandons fortement d'adopter cette approche quand vous modifiez JavaScript.

sitemods.js

Un squelette du fichier *sitemods.js* est distribué avec CA SDM. Il est inclus dans tous les fichiers HTMPL distribués, à la fin de leur section <head>, et est donc le dernier fichier JavaScript chargé. Par conséquent, toutes les fonctions qu'il définit remplacent toutes les fonctions de même nom précédemment chargées. Vous pourrez ainsi utiliser une version personnalisée d'une fonction JavaScript distribuée sans avoir à modifier directement le code distribué.

Cette méthode n'est cependant pas applicable aux fonctions invoquées au moment du chargement dans la section <head>, telles que celles de menubar.js et ahdmenus.js.

Vous pouvez cependant personnaliser la plupart des fonctions JavaScript en effectuant les opérations suivantes :

1. Placez une version modifiée de la fonction dans sitemods.js.
2. Stockez la copie mise à jour de sitemods.js dans CAisd/site/mods/www/wwwroot/scripts.

Informations complémentaires :

Modification de barres de menus (page 411)

Modification des menus contextuels

Certains formulaires CA SDM utilisent des menus contextuels, auxquels vous pouvez accéder en cliquant avec le bouton droit de la souris sur un objet. Vous pouvez modifier les menus contextuels grâce à Outil de conception Web qui vous permet d'ajouter, de supprimer ou de modifier les éléments de ces menus.

Remarque : Pour plus d'informations sur l'ajout d'éléments de menu, consultez l'*Aide de Outil de conception Web*.

Mise à jour et création d'ordres de changement en tant qu'utilisateur employé

Par défaut, un utilisateur peut seulement voir les ordres de changement à partir de l'interface Web Employé. Pour autoriser les employés à créer et à mettre à jour des ordres de changement, procédez comme suit :

1. Connectez-vous au Web en tant qu'Administrateur et sélectionnez l'onglet Administration.
2. Sélectionnez Type d'accès dans le menu Sécurité.

   La fenêtre Liste des types d'accès s'affiche.
3. Sélectionnez le lien Employé pour afficher la fenêtre de détail du type d'accès Employé.
4. Attribuez à Ordres de changement la valeur "modifier" sous l'onglet Accès Fonction, puis enregistrez.
5. Cliquez sur le bouton Précédent pour revenir à l'onglet Administration, puis sélectionnez Partition des données, Liste des partitions de données.
6. Cliquez sur Employé pour afficher la fenêtre Détail de la partition de données. Dans la partie Liste des contraintes de la fenêtre, consultez la colonne Type pour les tables Change_Request suivantes :
   - Mise à jour préalable
   - créer
7. Pour chaque table que vous souhaitez modifier, cliquez sur le nom de la table pour afficher la fenêtre Détail de la contrainte de partition de données de cette table.
8. Cliquez sur le bouton Modifier.
9. Modifiez la contrainte comme suit :

   Remplacez "id = 1" par "affected_contact = @root.id".
10. Cliquez sur Enregistrer.

Désormais, lorsque vous vous connecterez à l'interface Web en tant qu'utilisateur employé, le lien *Créer une demande de changement* s'affichera.

Ajout d'un lien Demandes de changement clôturées au tableau de résultats des employés

Vous pouvez utiliser ce produit pour ajouter une option de noeud Changements clôturés au tableau d'affichage de l'interface Web Employé.

Pour ajouter un noeud Changements clôturés, procédez comme suit :

1. Connectez-vous au produit en tant qu'administrateur.
2. Cliquez sur l'onglet Centre de services.

3. Sélectionnez Fichier, Personnaliser le tableau de résultats.

   La boîte de dialogue Personnaliser le tableau de résultats s'affiche.

4. Cliquez sur l'option Rôle et sélectionnez Employé dans la liste déroulante.

5. Sous Ajouter un nouveau noeud, cliquez sur le lien Requête stockée du noeud.

   La boîte de dialogue Liste des requêtes stockées s'affiche.

6. Faites une recherche et sélectionnez l'option Changements clôturés dans la liste des requêtes stockées. En général, cela s'affiche sous la forme du code CHGUBIN7.

7. Indiquez un emplacement pour le nouveau noeud en sélectionnant un élément dans l'arborescence du tableau d'affichage à gauche.

8. Cliquez sur Ajouter un noeud.

   Le nouveau noeud Changements clôturés est ajouté à l'arborescence du tableau d'affichage.

9. Cliquez sur Terminé.

Télécharger des pièces jointes

Lorsque vous téléchargez une pièce jointe dans CA SDM,, cette dernière est automatiquement affichée dans la fenêtre du navigateur sans aucune intervention de votre part. Cette action peut s'avérer dangereuse si un virus est associé à la pièce jointe.

Avec CA SDM, il est possible de forcer l'apparition d'une boîte de dialogue Enregistrer sous qui vous permet de préciser si vous souhaitez ouvrir la pièce jointe ou l'enregistrer sur le disque. Enregistrer une pièce jointe peut être une méthode sécurisée car vous pouvez enregistrer la pièce jointe sur le disque puis l'analyser avant de l'ouvrir. Vous avez également la possibilité de forcer l'affichage de la boîte de dialogue "Enregistrer sous" uniquement pour certains types de pièces jointes.

Il est possible de forcer l'apparition de la boîte de dialogue Enregistrer sous par le biais du fichier de configuration du servlet Web.xml. Le chemin du fichier Web.xml est le suivant :

Windows : $NX_Root\bopcfg\www\CATALINA_BASE\webapps\CAisd\WEB-INF\web.xml

Linux : $NX_ROOT est "/opt/CAisd"

Chapitre 9: Personnalisation du stockage des données du journal d'événements

La variable d'environnement système *@NX_EVENT_LOG_EXCLUDE*, qui est définie dans le fichier *NX.env* et requiert un redémarrage des services CA SDM, permet de contrôler la quantité de données stockée dans le journal d'événements (tableau event_log). Cette variable vous permet uniquement de stocker les événements pour lesquels vous voulez effectuer un suivi et établir un rapport, et que vous voulez utiliser dans le cadre de l'Activité récente pouvant être lancée en tant que bouton depuis la page de profil rapide.

Dans cette variable, des virgules séparent les éléments de liste (par exemple, *@NX_EVENT_LOG_EXCLUDE = FAQ,KD_OPEN*). Par exemple, si vous utilisez les événements LOGIN,LOGOUT de la table suivante (la valeur @NX_EVENT_LOG_EXCLUDE de LOGIN,LOGOUT), le produit n'enregistre pas les événements d'ouverture et de fermeture de session

Consultez les informations suivantes lorsque vous personnalisez des données que vous voulez stocker dans le journal d'événements à l'aide de cette variable :

Événement	Enum	Par	Jeux	commentaires
LOGIN	1	CA SDM		Spécifie que l'utilisateur se connecte système.
LOGOUT	2	CA SDM	numdata1	Spécifie que l'utilisateur ferme la session, où numdata1=raison de la fermeture de session : **0**-normal **1**-temporisation **2**-anormal
CR_CREATE	3	CA SDM	sd_ob_type, sd_obj_id, kd, numdata1	Indique que l'utilisateur crée un appel, où numdata1=id de l'utilisateur final concerné.
ISS_CREATE	4	CA SDM	sd_ob_type, sd_obj_id, kd, numdata1	Indique que l'utilisateur crée une demande de changement, où numdata1=id de l'utilisateur final concerné.
CHG_CREATE	5	CA SDM	sd_ob_type, sd_obj_id, kd, numdata1	Indique que l'utilisateur crée une demande client, où numdata1=id de l'utilisateur final concerné.

Événement	Enum	Par	Jeux	commentaires
EMAIL	6	Gestion des connaissances	kd	Spécifie que l'analyste envoie un document par courriel.
LINK	7	Gestion des connaissances	kd, sd_obj_type, sd_obj_id	Indique que l'utilisateur accepte une solution et la relie à un billet.
DEFAIRE UN LIEN	8	CA SDM	sd_id, sd_obj_type, sd_obj_id	Spécifie que l'utilisation supprime le lien entre une solution et un billet.
SEARCH	9	Gestion des connaissances	numdata1,	Indique que l'utilisateur effectue une recherche dans les connaissances, où numdata1= CI_ASKED_QUES id.
FAQ	10	Gestion des connaissances	numdata1	Indique une recherche FAQ, où numdata1= ID O_INDEXES (catégorie).
DT_ NAVIGATE	11	Gestion des connaissances	kd, numdata1, textdata1	Indique que l'utilisateur parcourt l'arborescence, où numdata1 = ID ES_NODES textdata1=path.
KD_ BOOKMARK	12	Gestion des connaissances	kd	Indique que l'utilisateur ajoute un document de connaissances aux favoris.
KD_ COMMENT	13	Gestion des connaissances	kd, numdata1	Indique que l'utilisateur ajoute un commentaire à un document de connaissances, où numdata1= ID O_COMMENTS.
KD_CREATE	14	Gestion des connaissances	sd_ob_type, sd_obj_id kd	Spécifie qu'un utilisateur crée un document. Les ID de CA SDM sont utilisés lors de la création d'un document de connaissances à l'aide de l'option Soumettre des connaissances à partir d'un appel ou d'une demande client.
KD_OPEN	15	Gestion des connaissances	kd, numdata1	Indique qu'un utilisateur ouvre un document de connaissances, où numdata1=ID BU_TRANS.
KD_RATE	16	Gestion des connaissances		Indique qu'un utilisateur classe un document de connaissances, où numdata1=ID BU_TRANS.

Événement	Enum	Par	Jeux	commentaires
KD_NEW	17	Gestion des connaissances	numdata1	Spécifie qu'un utilisateur clique sur dossier Nouveaux documents dans l'onglet Connaissances.
NX_ATTACH_ AUDIT_TO_NEW_TIC KET	18	CA SDM		Quand un utilisateur ouvre un nouveau billet, tous les événements de la session en cours s'affichent par défaut sur l'onglet Journal d'événements du billet. **0** — Seuls les événements se rapportant à ce billet figurent sous l'onglet Journal d'événements. **1** — Tous les événements de la session en cours figurent sous l'onglet Journal d'événements du billet.
TICK_OPEN	19	CA SDM		Indique que le billet était affiché.
TICK_SEARCH	20	CA SDM		Indique que l'utilisateur recherchant des billets et indique le nombre de recherches.
KD_PRNT	21	Gestion des connaissances	kd	Indique que le document de connaissances a été imprimé.

Personnalisation des Rapports CA Business Intelligence

Vous pouvez personnaliser les rapports CA Business Intelligence, en commençant à partir du point après lequel les champs et les tables ont été définis dans le schéma CA SDM.

Remarque : Pour de plus amples renseignements sur les modifications de schéma, reportez-vous à la section Aperçu des modifications à l'aide de l'outil de conception de schémas.

Avant de commencer, assurez-vous que vous avez effectué les opérations suivantes :

- Vous avez installé et configuré CA Business Intelligence de façon à ce qu'il fonctionne correctement avec CA SDM.
- Vous avez déterminé les autorisations utilisateur, les rôles, les options d'authentification et la sécurité des partitions de données pour votre environnement de signalement.

Remarque : Pour de plus amples renseignements sur la configuration de la sécurité de CA Business Intelligence, reportez-vous au *Manuel d'administration*.

Infrastructure de CA Business Intelligence

Le CA Business Intelligence (CA BI) est une infrastructure de signalement d'entreprise qui vous permet de créer, maintenir, stocker, planifier et distribuer des rapports pour les utilisateurs et les rôles de CA SDM. BusinessObjects Enterprise XI version 2 et ses objets, associé à BusinessObjects Crystal Reports XI, constitue l'épine dorsale de cette architecture. Les outils de BusinessObjects Enterprise, réunis dans une trousse créée par CA SDM, intègrent les éléments fondamentaux du signalement de CA SDM dans une structure d'aide à la décision de pointe.

Remarque : Bien que les rapports Crystal soient fournis comme composant principal de CA BI, l'outil de génération de rapports et de maintenance, Crystal Reports XI, n'est pas fourni. Crystal Reports XI est un produit avec licence séparée qui peut être acheté auprès de BusinessObjects et utilisé avec CA BI.

Composants de signalement

Les principaux composants de l'infrastructure de CA Business Intelligence sont les suivants :

- Base de données/Domsrvr/Pilote ODBC de **CA SDM** : les données de rapport sont stockées sur un serveur SQL ou dans une base de données CA SDM Oracle. Les applications de signalement de BusinessObjects (Crystal Reports et Web Intelligence) accèdent à la base de données à l'aide d'un pilote ODBC qui se connecte directement au moteur d'objets CA SDM (domsrvr). La sécurité CA SDM, y compris la partition de données et les restrictions de propriété, est automatiquement appliquée aux rapports.
- **Central Management Server :** le serveur CMS (Central Management Server) est le référentiel central qui stocke tous les objets utilisés dans chaque processus de signalement.
- **Central Management Console :** la console CMC (Central Management Console) est l'outil administratif principal de BusinessObjects. Il permet d'accéder à toutes les fonctions d'administration de BusinessObjects. En utilisant la CMC, vous pouvez déployer des rapports et affecter les accès utilisateur et les autorisations du dossier pour InfoView.

- **Univers BusinessObjects :** l'univers fournit une représentation commerciale d'un entrepôt de données ou d'une base de données transactionnelle. Il décrit les classes (tables) et les objets (colonnes) qui sont utilisés dans des rapports. L'univers de CA SDM est installé et configuré pendant l'installation. A l'achèvement de l'installation, la connexion de l'univers est affectée à divers groupes et utilisateurs dans CA SDM.
  - **Designer :** Designer (Outil de conception) est un outil de BusinessObjects Enterprise qui permet de modifier l'univers CA SDM, c'est-à-dire une métacouche entre le schéma CA SDM et les outils de signalement BusinessObjects. L'Assistant d'importation/d'exportation facilite le remplissage d'objets ou l'extraction d'objets dans le CMS.
- **Rapports prédéfinis par défaut :** les rapports prédéfinis sont des rapports Web CA SDM et Gestion des connaissances développés dans BusinessObjects Web Intelligence (WebI) ou Crystal Reports. Vous pouvez utiliser les rapports en tant que modèles pour définir des rapports spécifiques au site.
- **InfoView :** BusinessObjects InfoView est une interface Web qui permet aux utilisateurs CA SDM autorisés d'interagir avec des rapports Web prédéfinis en affichant, exécutant et planifiant des types de rapports, y compris, mais sans limitation, WebI et Crystal Reports. Les rapports sont contenus dans des dossiers de la section publique d'InfoView.
- **Rapports ad hoc :** les rapports ad hoc sont créés et administrés dans InfoView à l'aide d'une interface basée sur un module d'extension Web Intelligence. Cet outil est conçu pour les utilisateurs qui souhaitent créer des rapports de base facilement sans écrire de requêtes.

Environnement de développement

La mise à jour de l'infrastructure de CA BI avec des modifications de schéma de CA SDM est une fonction d'administration. Un administrateur qui promeut le schéma modifié dans les rapports doit configurer l'environnement, en dehors de leur environnement de production.

Certains des outils utilisés par CA BI requièrent une architecture Windows. Cela implique que les installations de Linux/UNIX doivent configurer CA BI sur un ordinateur Windows de façon à interagir avec l'installation CA BI de l'environnement de production de Linux/UNIX. Si vous utilisez des serveurs Windows dans la production, nous vous conseillons de configurer un ordinateur Windows supplémentaire pour votre environnement de développement.

Outils

La mise à jour de l'infrastructure de CA BI avec des modifications de schéma de CA SDM est une fonction d'administration. Pour promouvoir les modifications du schéma modifié dans les rapports, il faut inclure les outils suivants dans l'environnement de développement :

Business Objects Designer

Ce client Windows complet est installé sur le serveur de production de CA BI dans le cadre de l'installation de base de CA BI pour Windows. Lorsque le serveur CA BI utilise une architecture autre que Windows, ou lorsque la connexion au serveur d'applications CA BI de production n'est pas souhaitable, vous devez créer une installation de CABI distincte sur un serveur (de développement) Windows. L'installation d'un serveur CA BI de développement permet accéder à distance aux objets CA BI de production, quelle que soit l'architecture de l'installation du serveur de production CA BI.

BusinessObjects Web Intelligence

Cet outil Web de création de rapports est utilisé pour modifier et créer des rapports Web Intelligence (WebI). L'outil WebI est accessible par le biais de l'interface InfoView de BusinessObjects. Les droits d'administration sur les outils WebI et InfoView sont disponibles dans le CA BI ; ils sont accessibles par l'entremise de la console de gestion centrale (CMC) de BusinessObjects.

Pilote ODBC de CA SDM

Le pilote ODBC de CA SDM est inclus dans l'installation de CA BI. Ce composant permet à WebI et à Crystal Reports d'accéder à des données de CA SDM tout en appliquant la sécurité de la partition de données. Le pilote ODBC est installé dans le cadre de l'installation de base CA BI sur le serveur d'applications CA BI. Il est aussi disponible en tant que client installé, ce qui permet de l'utiliser sur un ordinateur qui n'exécute pas CA BI avec le client Crystal Reports XI.

Remarque : Pour plus d'informations sur la définition de la sécurité des partitions des données pour votre environnement de signalement, reportez-vous au *Manuel d'administration.*

Création d'un environnement de développement

Pour créer un environnement de développement, procédez comme suit :

1. Sécurisez un serveur avec un système d'exploitation Windows pris en charge.
2. Installez et configurez CA SDM.
3. Installez et configurez CA Business Intelligence.

4. Remplacez le nom de l'ODBC DSN par défaut casd_xxxxx par casd_yyyyy, yyyyy correspondant exactement au DSN sur la mise en oeuvre de production.

   Important : Quelles que soient les propriétés réelles de la connexion, le nom du DSN doit être identique sur les mises en oeuvre de développement et de production.

5. (Facultatif) Installez et configurez Crystal Reports XI.

   Remarque : Il n'est pas obligatoire d'installer Crystal Reports sur le même ordinateur que CA BI. Il est possible d'installer Crystal Reports sur un autre ordinateur à condition que le pilote ODBC de CA SDM soit aussi installé sur l'ordinateur où se trouve Crystal Reports et que le nom du DSN soit modifié de façon à être identique à la mise en oeuvre de production, quelles que soient les propriétés de connexion réelles. Pour plus d'informations sur l'installation d'une copie du pilote ODBC de CA SDM, distincte de l'installation CA BI, reportez-vous à la documentation du pilote ODBC.

6. Créez le cadre (page 504).

Environnement

Une fois les outils disponibles dans votre environnement de développement, l'étape suivante consiste à créer un cadre qui permettra de conserver les modifications de schéma lors des mises à niveau du produit.

Important : Ne modifiez pas l'univers de développement CA SDM par défaut installé avec CA BI, sinon vos modifications de schéma risquent d'être écrasées pendant les processus de mise à niveau et d'installation des correctifs. Modifier l'univers de CA SDM finit par entraîner la perte des modifications de schéma dans l'infrastructure de CA BI.

L'univers BusinessObjects est la métacouche qui décrit le schéma dans l'infrastructure de CA BI. Au lieu de modifier l'univers CA fourni, vous pouvez créer un univers spécifique à un client relié à l'univers de CA SDM. Cette approche vous permet de conserver les modifications de schéma locales avec un minimum d'efforts lors du processus de mise à niveau et CA SDM pourra fournir des mises à niveau à l'univers de base.

Les clients de CA SDM familiarisés avec la documentation de l'univers BusinessObjects savent qu'il existe des procédures établies pour BusinessObjects qui permettent de relier des univers entre eux. Néanmoins, le processus présenté ici est le seul qui est pris en charge par CA pour conserver les modifications des clients.

L'univers par défaut s'appelle CA SDM. Il est stocké dans le dossier CA Universes de la console de gestion centrale (CMC). Cet univers par défaut est l'univers "noyau" dans une structure où les univers sont reliés.

Vous pouvez donner le nom que vous voulez à l'univers de CA SDM. C'est le nom que verront les créateurs de rapports quand ils créeront des rapports, alors assurez-vous qu'il est significatif. L'univers client est l'univers "dérivé" dans une structure où les univers sont reliés.

Il est possible de conserver de nombreux univers dérivés dans cet environnement, mais un seul est nécessaire pour conserver les modifications de schéma. Vous pouvez utiliser plusieurs univers dérivés pour faciliter la maintenance ou pour répondre aux exigences de sécurité, mais ce genre de décision dépend exclusivement de vos besoins en matière de prise en charge de production.

Dans tout environnement comportant plusieurs univers dérivé, veillez à procéder comme suit :

- Préservez la convention d'attribution de nom z_ pour le nom du fichier d'univers de tous les univers.
- Utilisez la connexion à CA SDM, puis stockez l'univers dans le dossier CA Customer Universe.
- Ne supprimez pas le lien vers l'univers noyau.

Création d'une structure pour promouvoir les modifications de schéma dans CABI

Utilisez BusinessObjects Designer pour créer un cadre pour la promotion des modifications de schéma dans CA Business Intelligence.

Pour créer un cadre de promotion des modifications de schéma :

1. Ouvrez BusinessObjects Designer.

   Dans le menu de Designer, sélectionnez File, New.

   La fenêtre Universe Parameters s'affiche.

2. Cliquez sur l'onglet Definition et entrez un nom significatif pour cet univers dans le champ Name.
3. (Facultatif) Entrez une description dans le champ Description.
4. Sélectionnez CA SDM dans la liste déroulante Connection.
5. Cliquez sur le bouton Add Link de l'onglet Links.

   La boîte de dialogue Universe to Link (Univers à relier) s'affiche.

6. Développez le dossier CA Universes et effectuez les tâches suivantes.

   a. Ouvrez le fichier CA Service Desk.unv. La boîte de dialogue Universe to Link (Univers à relier) se ferme et l'univers de CA SDM apparaît sur l'onglet Liens.

   b. Cliquez sur OK pour fermer la boîte de dialogue Universe Parameters.

   Designer peut prendre quelques minutes pour traiter le lien et créer l'univers dérivé.

7. Une fois l'univers dérivé créé, exécutez les tâches suivantes.
   a. Modifiez le(s) paramètre(s) suivant(s) de manière appropriée.
      - Dans le menu File, sélectionnez Parameters.
      - Cliquez sur l'onglet Parameter.
      - Spécifiez ANSI92 = YES.
   b. Cliquez sur l'onglet Controls et définissez les champs suivants sur une valeur adaptée à votre mise en oeuvre, puis cliquez sur OK pour enregistrer les valeurs et fermer la boîte de dialogue de paramètres :
      - Limit size of result set
      - Limit execution time
      - Limit size of long text objects (minimum of 4000).
   c. Définissez des hiérarchies. Remarque : Les hiérarchies client ne sont pas importées.
      - Sélectionnez Tools, Hierarchies.
      - Effectuez une sélection multiple de toutes les hiérarchies personnalisées, puis cliquez sur la flèche Add. Toutes les hiérarchies sont déplacées dans la liste de droite.
8. Dans le menu de Designer, cliquez sur File, Save.

   La boîte de dialogue Enregistrer sous apparaît.
9. Dans le champ File Name, sélectionnez un nom de fichier descriptif et faites précéder le nom du fichier par "z_". Par exemple, un univers nommé "ACME Anvil Co" est nommé par défaut : "ACME_Anvil_Co.unv". Remplacez ce nom de fichier par "z_ACME_Anvil_Co.unv" avant d'enregistrer.
10. Exportez l'univers dérivé vers le CMS comme suit :
    a. Dans le menu de Designer, sélectionnez File, Export.
    b. Dans la liste déroulante de champ Domain, sélectionnez <Browse>, puis recherchez et sélectionnez CA Customer Universes.
    c. Cliquez sur OK pour exporter l'univers vers le serveur CMS local.

       La boîte de dialogue Univers exporté avec succès apparaît.

    La structure existe désormais pour promouvoir les modifications de schéma personnalisé dans tout CA BI.
11. Connectez-vous à BusinessObjects InfoView en tant qu'utilisateur administratif et effectuez les actions suivantes.
    a. Sélectionnez Public Folders.
    b. Dans la barre d'outils d'InfoView, cliquez sur New, Folder.

c. Dans le champ Folder Name, fournissez une description pertinente pour les utilisateurs du rapport, comme "Rapports des noms d'organisation".

d. Cliquez sur OK pour voir le dossier créé s'afficher sous Public Folders.

Cela crée la structure minimale pour utiliser et stocker les rapports créés par votre organisation. Un nombre illimité de sous-dossiers et d'objets peuvent être ajoutés à cette structure de dossiers.

Modifications de schéma dans l'Infrastructure

Une fois que l'environnement de développement de CA BI est établi et que les modifications de schéma ont été publiées dans CA SDM à l'aide du processus de personnalisation des données de schéma documenté, les modifications de schéma sont prêtes à être promues dans l'infrastructure CA BI. Vous pouvez rendre le nouveau schéma disponible pour la création et la modification de rapports.

Ajouter des modifications de schéma à l'univers dérivé

Le processus de promotion des modifications de schéma dans l'infrastructure CA est aussi simple que celui consistant à ajouter le nouvel objet de schéma à l'univers dérivé.

Remarque : Avant de commencer, assurez-vous que les étapes appropriées ont bien été suivies et que les nouveaux objets de schéma ont été ajoutés au schéma flexible de CA SDM.

Pour ajouter des modifications de schéma à l'univers dérivé, procédez comme suit :

1. Ouvrez BusinessObjects Designer et importez l'univers dérivé dans un système de fichiers local de la façon suivante :

   a. Dans le menu Outil de conception, sélectionnez Fichier, Importer.

      La boîte de dialogue Universe successfully imported s'affiche.

   b. Cliquez sur OK.

2. Actualisez la structure de l'univers dérivé comme suit :

   - Dans le menu Outil de conception, sélectionnez Afficher, Refresh structure (Actualiser la structure).

     Les questions suivantes s'affichent :

     - Do you want to refresh the out of date columns in selected tables? (Voulez-vous actualiser les colonnes obsolètes dans les tables sélectionnées) Cliquez sur OK.

     Remarque : Si le message "No update needed" (Aucune mise à jour nécessaire) s'affiche, cela signifie que la couche objets de CA SDM n'a pas été mise à jour correctement avec le nouveau schéma. Consultez les étapes de publication des modifications de schéma de CA SDM.

- Refresh structure (Actualiser la structure) : The structure has been successfully modified. (La structure a été modifiée avec succès.) Cliquez sur OK.

Les nouvelles colonnes apparaissent dans la structure de l'univers sur le côté droit de la fenêtre, ce qui rend les nouveaux objets disponibles et permet leur utilisation dans l'univers dérivé.

Les objets sont à la disposition des outils de CA BI après avoir été déplacés du volet droit vers le volet gauche. Quand vous ajoutez des objets au volet gauche, veillez à respecter les normes communes de modification de schéma (page 508).

3. Faites glisser et déposez les nouveaux objects à l'emplacement voulu dans le volet gauche.
4. Cliquez sur Enregistrer.
5. Dans le menu de Designer, sélectionnez File, Export.

   La boîte de dialogue Univers exporté avec succès apparaît.
6. Cliquez sur OK.

   Les modifications ajoutées au schéma d'univers dérivé sont exportées vers le CMS local.
7. Dans le menu Outil de conception, sélectionnez Outils, Vérifier l'intégrité.
   a. Dans la boîte de dialogue qui s'affiche, cochez la case correspondant à l'analyse des objets. (Ne modifiez pas d'autre paramètre.)
   b. Cliquez sur OK. Le contrôle d'intégrité commence.

      Remarque : Aucune erreur d'analyse ne doit être signalée. Si des erreurs sont détectées, modifiez vos objets dans le volet gauche pour éviter les erreurs d'analyse.
8. Cliquez sur OK pour fermer la boîte de dialogue.
9. Exportez l'univers dérivé vers le CMS comme suit :
   a. Dans le menu de Designer, sélectionnez File, Export.
   b. Dans la liste déroulante du champ Domaine, sélectionnez <Parcourir>, puis localisez et sélectionnez les univers clients de CA.
   c. Cliquez sur OK pour exporter l'univers vers le CMS local.

   La boîte de dialogue Univers exporté avec succès apparaît.
10. Enregistrez vos modifications et exportez l'univers de CA SDM.

    Les modifications sont maintenant disponibles dans votre environnement de signalement de CA BI, y compris dans Web Intelligence et Crystal Reports.

Modifications de schéma commun

Vous pouvez mettre en oeuvre des modifications de schéma dans l'univers. Pour vous familiariser avec ce processus, le tableau ci-dessous répertorie les modifications de schéma communes que vous pouvez rencontrer.

Quand un type de champ est défini dans l'outil de conception Web en tant que...	**Suivez ces règles lorsque vous utilisez ce champ dans l'univers : Cliquez avec le bouton droit de la souris sur l'attribut et sélectionnez...**
INTEGER	Propriétés de l'objet, Onglet Définition, Type = Nombre
CHAINE	Propriétés de l'objet, Onglet Définition, Type = Caractère
DATE	Propriétés de l'objet, Onglet Définition, Type = Date Format de l'objet, Onglet Nombre : Choisissez la catégorie "Date/Heure" ; Choisissez le format dd/mm/yyyy hh:mm:ss AM/PM
DUREE	Propriétés de l'objet, Onglet Définition, Type = Nombre ; Propriétés de l'objet, Onglet Définition, Sélectionnez = PdmSeconds(object.attr)
SREL	Créez un alias d'attribut CA SDM.
BREL	(Non applicable)
QREL	(Non applicable)
DERIVEE	Utilisez un type de données et un format d'objet appropriés pour la valeur stockée dans le champ dérivé. Le champ Dérivée peut produire n'importe quel résultat, de sorte qu'il n'existe pas de norme particulière à respecter.
Cas particulier : Local Il ne s'agit pas d'un type de données défini dans l'Outil de conception Web, mais plutôt d'un type de données utilisé parfois dans l'univers pour indiquer un type de données qui n'est pas pris en charge.	Le champ Local est affiché dans le volet droit de l'univers, accompagné du type L. Il est possible de faire glisser ces champs, mais pas de les déposer dans une classe du volet droit de l'univers. Le plus souvent, les types de données de champs, tels que le type binaire, ne sont pas pris en charge par l'univers. Il est cependant possible de les ajouter au volet gauche de l'univers en créant un objet et en plaçant le PdmString (object.attribute) dans la fenêtre de sélection de la boîte de dialogue de modification des propriétés.

Structures de dossiers et de rapports

Plusieurs objets de rapports Crystal Report XI et WebI sont inclus dans l'installation de CA BI. Ces rapports sont réunis dans le dossier de CA SDM suivant : CA Reports\CA SDM.

Important : Ne modifiez pas l'univers de CA SDM et les objets de rapport contenus dans la structure de dossiers de CA SDM.

Tenez compte des informations suivantes sur les rapports et les structures de dossiers :

- La méthodologie de création d'un cadre explique comment ajouter un dossier dans la section publique d'InfoView, qui est spécifique à l'utilisateur final. Dans ce dossier, un utilisateur peut créer des sous-dossiers et objets de rapport supplémentaires.
- Dans une mise en oeuvre où chaque utilisateur est autorisé à accéder à CA BI à l'aide de son ID de connexion unique à CA SDM, les utilisateurs peuvent enregistrer des rapports destinés à leur usage personnel dans la section My Folders. BusinessObjects fait respecter la sécurité sur ce dossier en ne présentant ces objets qu'à l'utilisateur connecté.
- Dans une mise en oeuvre où tous les utilisateurs utilisent un même ID d'utilisateur de signalement pour accéder à CA BI, la section My Folders est accessible à tous les utilisateurs.

Création d'un rapport de Web Intelligence

Utilisez CA Business Intelligence pour créer un rapport Web Intelligence.

Pour créer un rapport Web Intelligence :

1. Dans l'onglet Rapports de CA SDM, cliquez sur le bouton InfoView.

   La page d'accueil de InfoView apparaît.

2. Cliquez sur New, Web Intelligence Document dans la barre de menus.

3. Sélectionnez l'univers dérivé que vous avez créé lorsque vous avez défini votre cadre de développement.

   L'outil de création de rapports de Web Intelligence s'affiche.

   Remarque : Enregistrez régulièrement votre document. Si la session de connexion expire, vos modifications de rapports seront perdues. Pour plus d'informations sur l'augmentation de la valeur de temporisation de la session de connexion de Web Intelligence, reportez-vous au *Manuel d'administration*.

4. Dans la barre d'outils de Web Intelligence, sélectionnez Enregistrer, Enregistrer sous.

   La boîte de dialogue Save Document (Enregistrer le document) s'affiche.

5. Dans la section Général, entrez un nom significatif pour ce rapport dans le champ Titre.
6. Dans la section Emplacement, sélectionnez le dossier approprié.
7. (Facultatif) Modifiez les propriétés comme vous le souhaitez.
8. Cliquez sur OK pour enregistrer le rapport.

   Le rapport apparaît dans le dossier spécifié et il est mis à la disposition de tous les utilisateurs de rapports.

Modifier un rapport de Web Intelligence

Pour modifier un rapport qui a été distribué dans la structure de dossiers CA Reports\CA Service Desk, utilisez CA Business Intelligence.

Pour modifier un rapport CA Business Intelligence :

1. Dans l'onglet Rapports de CA SDM, cliquez sur le bouton InfoView.

   La page d'accueil de InfoView apparaît.
2. Dans le volet gauche, naviguez jusqu'à la structure de dossiers CA Reports et ouvrez le rapport de Web Intelligence désiré.
3. Cliquez sur le nom du rapport pour qu'il s'exécute et affiche un résultat.
4. Dans la barre d'outils de Web Intelligence, sélectionnez Document, Enregistrer sous.

   La fenêtre d'enregistrement du document s'ouvre.
5. Dans la section Emplacement, sélectionnez le dossier approprié.
6. Cliquez sur OK pour enregistrer le rapport dans le nouvel emplacement.
7. Sélectionnez Document, Modifier.
8. Cliquez sur Edit Query (Modifier la requête) (le nom de l'univers de CA SDM apparaît sur l'onglet Données).
9. Cliquez sur l'onglet Propriétés. Si nécessaire, cliquez sur la flèche orientée vers le bas située à côté de l'univers afin que le texte CA SDM s'affiche avec des points de suspension (...).
10. Cliquez sur les points de suspension (...) afin d'afficher la boîte de dialogue Univers.

    La fenêtre Other Available Universes (Autres univers disponibles) s'affiche.

11. Sélectionnez le nom de votre univers et cliquez sur OK.

    Web Intelligence mappera automatiquement tous les champs connus de l'univers de CA SDM à votre univers et affichera la boîte de dialogue Change Source (Modifier la source). Des cases à cocher vertes apparaissent à côté de chaque champ mappé. Si tous les champs sont mappés correctement, cliquez sur OK pour confirmer la modification. Si un champ s'affiche accompagné d'un X rouge, cliquez sur les points de suspension (...) situés à côté du nom du champ et sélectionnez le champ approprié.

12. Dans la barre d'outils de Web Intelligence, cliquez sur Edit Report (Modifier le rapport) et sélectionnez l'onglet Propriétés.

13. Développez le noeud Général.

14. Cliquez sur les points de suspension (...) à côté de la valeur Propriétés du document.

    La boîte de dialogue Propriétés du document s'affiche.

15. Dans la section des options du document, cochez la case Refresh on Open (Actualiser à l'ouverture).

16. Cliquez sur Enregistrer et fermez Web Intelligence.

    Le rapport est associé avec l'univers approprié et peut être modifié comme il convient.

Création d'un rapport Crystal

Utilisez des rapports Crystal pour enregistrer un rapport dans l'univers CA Business Intelligence.

Pour créer un rapport Crystal

1. Lancez Crystal Reports XI.

2. Sélectionnez Fichier, Nouveau, Rapport vide.

   La boîte de dialogue Personne spécialiste des bases de données apparaît.

3. Développez le noeud Create new Connection (Créer une nouvelle connexion) et cliquez sur Univers.

   La boîte de dialogue de Businessobjects Enterprise s'affiche.

4. Connectez-vous à BusinessObjects Enterprise en utilisant vos informations d'identification administrateur.

5. Accédez au dossier contenant l'univers dérivé.

6. Sélectionnez l'univers dérivé et cliquez sur Ouvrir.

   La boîte de dialogue relative au panneau d'interrogation de Business Objects s'affiche.

7. Dans l'arborescence de l'univers, faites glisser et déposez les attributs appropriés dans les sections de sélection et de filtrage du panneau de requête.
8. Une fois le processus de construction de requête terminé, l'outil de conception standard de Crystal Reports s'affiche.
9. Générez et exécuter le rapport

   Remarque : Pour plus d'informations sur la création et l'exécution de rapports, reportez-vous à la documentation de Crystal Reports.
10. Enregistrez le rapport dans le référentiel de Business Objects Enterprise comme suit :
    a. Sélectionnez Fichier, Enregistrer sous.
    b. Dans la boîte de dialogue Enregistrer sous, sélectionnez Entreprise.
    c. Accédez au dossier créé lorsque vous avez défini votre cadre de développement et enregistrez le nouveau rapport dans BusinessObjects Enterprise.

    Le nouveau rapport est maintenant disponible dans l'entreprise et peut être modifié si nécessaire.

Modification d'un rapport Crystal

Utilisez des rapports Crystal pour modifier un rapport dans l'univers CA Business Intelligence.

Pour modifier des rapports Crystal Reports XI

1. Ouvrez des rapports Crystal XI.
2. Sélectionnez Fichier, Nouveau, Rapport vide.

   La boîte de dialogue Personne spécialiste des bases de données apparaît.
3. Cliquez pour développer Créer une nouvelle connexion.

   Cliquez sur Univers.

   La boîte de dialogue Business Objects Enterprise s'affiche.
4. Connectez-vous à Business Objects Enterprise en tant qu'administrateur.

5. Cliquez pour accéder au dossier contenant l'univers dérivé, puis cliquez sur cet univers pour le sélectionner.

   Cliquez sur Ouvrir.

   La boîte de dialogue relative au panneau d'interrogation de Business Objects s'affiche.

6. Parcourez l'arborescence pour rechercher, faire glisser et déposer les attributs dans les sections de sélection et de filtrage du panneau d'interrogation.

   Une fois le processus de génération de la requête terminé, l'outil de conception standard de Crystal Reports est présenté au rédacteur du rapport.

7. Générez et exécutez le rapport conformément aux instructions de Crystal Reports.

8. Lorsque vous êtes prêt, enregistrer le rapport dans le référentiel de Business Objects Enterprise.

   a. Sélectionnez Fichier, Enregistrer sous.

      La boîte de dialogue Enregistrer sous s'affiche.

   b. Sur le côté gauche de la boîte de dialogue Enregistrer sous, cliquez sur l'icône Enterprise.

   c. Parcourez la structure des dossiers en commençant par le dossier spécifique au client créé précédemment dans ce document et cliquez sur Enregistrer pour enregistrer ce rapport dans Business Objects Enterprise.

9. Le nouveau rapport est maintenant disponible dans l'entreprise et peut être modifié si nécessaire.

Déplacer des nouveaux rapports Crystal dans CA Business Intelligence

Vous pouvez déplacer des rapports Crystal vers un univers CA Business Intelligence.

Pour déplacer de nouveaux rapports Crystal dans CA Business Intelligence

1. Ouvrez des rapports Crystal XI.

2. Sélectionnez Fichier, Ouvrir.

   La boîte de dialogue Ouvrir saffiche.

3. Sur le côté gauche, cliquez sur Enterprise.

   La boîte de dialogue Connexion à BusinessObjects Enterprise s'affiche.

4. Connectez-vous à BusinessObjects Enterprise en utilisant vos informations d'identification administrateur.

   Parcourez la structure des dossiers en commençant par CA Reports\CA Service Desk jusqu'à ce que le rapport cible s'affiche.

5. Sélectionnez le rapport cible et cliquez sur Ouvrir.

   Le rapport apparaît dans Crystal Reports.

6. Cliquez sur Fichier, Enregistrer sous.

   La boîte de dialogue Enregistrer sous apparaît.

7. Spécifiez le dossier que vous avez créé lorsque vous avez défini vote cadre de développement.

8. Cliquez sur Enregistrer.

9. Dans le menu Crystal Reports, sélectionnez Base de données, Personne spécialiste des bases de données.

   La boîte de dialogue Personne spécialiste des bases de données apparaît.

10. Dans le volet gauche, sélectionnez Créer une nouvelle connexion, Univers.

11. Sélectionnez l'univers dérivé.

12. Placez tous les attributs utilisés par ce rapport dans la nouvelle requête à l'aide d'un glisser-déposer, puis cliquez sur OK.

13. Dans chaque formule et chaque cellule, remplacez les attributs d'origine par ceux de la nouvelle requête.

14. Une fois tous les attributs remplacés, procédez de la manière suivante :

    a. Dans le menu Crystal Reports, sélectionnez Base de Données, Personne spécialiste des bases de données.

    b. Dans la boîte de dialogue Personne spécialiste des bases de données, sélectionnez la requête d'origine et cliquez sur les flèches dirigées vers la gauche au milieu des deux volets pour supprimer l'ancienne requête.

       - Si tous les attributs ont correctement été remplacés, la requête d'origine sera supprimée sans problème et vous pourrez continuer à modifier le rapport.

       - S'il reste un attribut d'origine dans le rapport un message indiquant que le rapport utilise des champs provenant de plusieurs tables et demandant si vous voulez poursuivre s'affiche.

       - Cliquez sur Annuler et revenez au rapport.

       - Continuez à remplacer tous les attributs d'origine par les attributs de la nouvelle requête jusqu'à ce que la requête d'origine puisse être supprimée sans générer de message d'avertissement.

    Le rapport est prêt à être personnalisé.

Déplacement des rapports d'accès existants dans CA Business Intelligence

Les rapports prédéfinis Microsoft Access ne sont plus développés ou fournis avec CA SDM. Vous pouvez cependant déplacer vos rapports Access existants dans l'environnement de signalement de CA Business Intelligence en procédant comme suit :

1. Ajoutez les modifications de schéma CA SDM appropriées à CA Business Intelligence.
2. Servez-vous de Web Intelligence ou de Crystal Reports pour réécrire le rapport.

Déplacement du développement à la production

A ce stade, un univers dérivé a été ajouté, des structures de dossiers ont été créées et des rapports ont été créés et modifiés. Par conséquent, vous pouvez déplacer la structure de développement vers la production. Dans cette étape, vous allez utiliser l'assistant d'importation de BusinessObjects.

Pour passer du développement à la production

1. Dans le menu Démarrer, sélectionnez Tous les Programmes, BusinessObjects XI version 2, BusinessObjects Enterprise, Assistant d'importation.

   L'interface de l'assistant d'importation s'affiche.

2. Dans la fenêtre Source Environment (Environnement d'origine), sélectionnez Business Objects XI R2 et fournissez les informations d'identification requises par le système de développement.

3. Sur l'écran Environnement Destination, sélectionnez *l'une* des options suivantes :

   - **Le système de production**. Cette option déplace immédiatement tous les objets sélectionnés dans le système de production.
   - **Un fichier externe pouvant être importé ultérieurement dans le système de production**. Cette option stocke tous les objets dans un fichier Business Intelligence Archive Resource (BIAR).

4. Dans l'écran Select Objects to Import (Sélectionner les objets à importer), effacez tous les paramètres et cochez les cases Import folders and objects (Importer des dossiers et des objets) et Import Universes (Importer des univers).

   Remarque : Ignorez les éventuels avertissements qui s'affichent.

5. Sélectionnez la structure de dossiers contenant votre dossier spécifique et désélectionnez tout objet qui ne doit pas être déplacé.

6. Dans l'écran Import Options for Universes and Connections (Importer des options pour les univers et les connexions), cliquez sur l'option Import the universes and connections that the selected Web Intelligence and Desktop Intelligence documents use directly (Importer les univers et les connexions que les documents Web Intelligence et Desktop Intelligence sélectionnés utilisent directement).

7. Dans le dossier et dans l'écran Univers, développez le dossier approprié contenant l'univers.

   Remarque : Ignorez les éventuels avertissements qui s'affichent.

8. Cliquez sur Terminer.

   Si les dossiers et les rapports ont été directement déplacés vers l'ordinateur de production, vous pouvez afficher les modifications dans InfoView. Si les objets ont été placés dans un fichier .biar, utilisez l'assistant d'importation plus tard, en sélectionnant le fichier .biar en tant qu'environnement d'origine et le serveur de production en tant qu'environnement de destination.

Personnalisation des rapports hérités

CA SDM vous permet de personnaliser des rapports hérités ou de concevoir vos propres rapports. Vous pouvez :

- personnaliser les rapports récapitulatifs, détaillés et d'analyse existants pour qu'ils contiennent exactement les informations dont vous avez besoin, par exemple des champs supplémentaires ;
- produire un nouveau rapport avec les informations disponibles dans la base de données dans un format qui vous convient ;
- transmettre les informations variables du rapport en incluant des arguments de ligne de commande ; les arguments peuvent correspondre à des valeurs ou à des expressions, par exemple la valeur actuelle d'un champ ou une expression de clause SQL WHERE ;
- générer des rapports à partir d'une ligne de commande, d'un fichier script ou d'une option de menu.

Pour générer un rapport personnalisé

1. Concevoir le rapport :
   - Déterminer quelles données vous souhaitez inclure dans le rapport.
   - Créez un modèle de rapport contenant des requêtes, expressions et fonctions de type SQL pour manipuler les données, et des instructions pour mettre en forme les données sur la page imprimée.

2. Générer le rapport depuis :
   - la ligne de commande ;
   - une option de menu d'CA SDM ;
   - un fichier script.

Remarque : Si vous disposez d'un système de base de données tiers, vous pouvez utiliser ses outils de génération de rapports pour créer des rapports avec des données provenant de la base de données CA SDM. CA SDM fournit plusieurs vues de base de données qui simplifient le processus de création de rapports personnalisés à l'aide de systèmes de bases de données tiers. Pour de plus amples renseignements sur le signalement, reportez-vous à la documentation de votre SGBD. Pour de plus amples renseignements sur les vues de base de données, reportez-vous au *Manuel d'administration*.

Renseignements supplémentaires :

Personnalisation des rapports Crystal (page 541)

Conception de rapport personnalisés

Pour concevoir un rapport personnalisé, vous devez avoir des connaissances de base sur les concepts suivants :

- écriture de requêtes SQL ;
- programmation, notamment en langage C ;
- création de programmes spécifiques ou de fichiers script à exécuter éventuellement avant le programme de modèle de rapport ; vous pouvez par exemple créer un programme invitant l'utilisateur à entrer un argument, tel que les conditions d'une clause WHERE.

Remarque : Avant de créer un rapport personnalisé, vérifiez que le rapport dont vous avez besoin existe déjà. CA SDM offre un vaste choix de rapports Crystal et Microsoft Access, de même que des versions d'exécution de ces produits pour vous permettre de générer les rapports. Pour plus d'informations sur les rapports, reportez-vous au *Manuel d'administration*.

Sélection d'informations pour le rapport

Pour plus d'informations sur la sélection de données provenant de la base de données CA SDM pour les rapports personnalisés, reportez-vous au *Manuel de référence technique* de *CA SDM*. Cette annexe répertorie les tables, les champs, les descriptions et d'autres informations de la base de données.

Création d'un modèle de rapport

Un modèle de rapport est un fichier qui, lorsqu'il est exécuté par un programme de rapport CA SDM, génère un rapport avec une mise en page spécifique. Un modèle de rapport contient des expressions de variables, des fonctions et des instructions définissant la manière dont les données sont extraites, calculées et imprimées.

Pour créer un modèle de rapport, créez un fichier contenant les types d'instructions suivants :

Instructions de bloc

Elles définissent les tables de la base de données CA SDM dans lesquelles les données sont extraites, ainsi que les actions à effectuer sur ces données.

Instructions de mise en page

Elles définissent la manière dont les variables de données et le texte littéral s'affichent dans le rapport.

Remarque : Stockez tous vos fichiers .rpt dans un nouveau répertoire, tel que $NX_ROOT/site/mods/rpt (UNIX) ou *répertoire-installation*\site\mods\rpt (Windows). Ce répertoire les conservera lorsque vous installerez une version plus récente de CA SDM.

Informations complémentaires :

Référence d'un modèle de rapport (page 526)
Exemple : Modèle de rapport (page 522)

Instructions de bloc

Les instructions de bloc permettent de définir la structure d'un modèle de rapport. Elles permettent de définir les données à manipuler et de contrôler l'exécution de ce rapport. Les instructions de bloc commencent par un nom qui doit être unique pour tout le modèle de rapport. Elles contiennent les deux sections suivantes :

Section de requête de données

Elle contient les clauses SQL SELECT, WHERE et SORT permettant de définir les données à extraire de la base de données.

Section de programme de sortie

Elle définit les actions à effectuer sur les données extraites. Elle contient des déclarations de variable, des fonctions et autres instructions de bloc, y compris des instructions imbriquées permettant de créer des rapports conditionnels. Elle peut également contenir des instructions de mise en page permettant de mettre en forme et d'imprimer les données sous forme de texte ASCII.

L'exemple suivant constitue une version simplifiée de la syntaxe d'une instruction de bloc illustrant la relation entre les deux sections :

```
BLOCK nom_block ("clause SELECT", "clause WHERE")

   Clause SORT {instructions du programme de sortie}
```

La rubrique relative à l'instruction BLOCK (page 533)de la section Référence fournit un exemple de syntaxe détaillée, ainsi qu'une description de chaque clause et de chaque paramètre.

Instructions de mise en page dans les modèles de rapport

Les instructions de mise en page définissent la manière dont les variables de données et le texte littéral s'afficheront dans le rapport.

- Les instructions PAGE HEADER et PAGE FOOTER permettent de placer des informations en haut et en bas de chaque page du rapport.
- Vous pouvez imbriquer des instructions HEADER, HEADER2, FOOTER et PRINT dans la section entre accolades de l'instruction BLOCK parent pour créer des titres et des totaux récapitulatifs pour les différentes *sections de signalement* (parties du rapport).

  Remarque : Lors de l'imbrication, ne confondez pas les accolades utilisées dans les instructions de mise en page et celles qui entourent les instructions imbriquées à l'intérieur d'une instruction BLOCK parent.
- Vous pouvez inclure du texte littéral pour créer des étiquettes ainsi que des caractères de tracé de ligne pour améliorer la présentation du rapport.

Les instructions de mise en page sont les suivantes :

PAGE HEADER

Place des informations en haut de chaque page du rapport. Elle est placée à l'extérieur de l'instruction BLOCK.

PAGE FOOTER

Place des informations en bas de chaque page du rapport. Elle est placée à l'extérieur de l'instruction BLOCK.

HEADER

Place des informations en haut de chaque section de signalement. Elle est placée à l'intérieur de l'instruction BLOCK.

HEADER2

Place la suite des informations d'en-tête en haut de chaque page consécutive d'une section de signalement si cette section couvre plusieurs pages. Elle est placée à l'intérieur de l'instruction BLOCK.

FOOTER

Place des informations en bas de chaque section de signalement. Elle est placée à l'intérieur de l'instruction BLOCK.

PRINT

Place les données dans une section de signalement. Elle est placée à l'intérieur de l'instruction BLOCK.

Vous pouvez également utiliser les variables prédéfinies suivantes dans les instructions de mise en page :

- La variable CT imprime l'heure actuelle.
- La variable CD imprime la date actuelle.
- La variable PG imprime le numéro de page.

Champs de données

Spécifie une variable dans une instruction de mise en page qui aboutit à un élément de données quand vous générez le rapport. Observez les recommandations suivantes lorsque vous placez des champs dans votre modèle de rapport :

- Mettez les champs de données entre crochets ([ ]).
- Les crochets du champ définissent sa largeur d'impression sur chaque ligne en sortie. Cette largeur correspond au nombre de caractères délimité par les crochets, crochets compris. Si le résultat d'une variable dépasse la largeur d'impression, la sortie est tronquée. Pour vous assurer que la largeur d'impression d'un champ est suffisante, vous pouvez ajouter des espaces entre le nom de la variable et le crochet fermant. Ces espaces permettent par exemple d'inclure des contacts ayant des noms longs :

```
[contact          ]
```

- Pour une sortie contenant moins d'une ligne, le champ peut être fermé par un chevron fermant (>). La largeur d'impression s'étend alors jusqu'à la marge de droite. Par exemple, le chevron fermant utilisé dans une instruction HEADER permet d'imprimer la date actuelle sans que celle-ci soit tronquée :

  ```
  [CD                >
  ```

  Remarque : Lorsque le champ contient plusieurs lignes et que la variable est marquée comme étant MULTILINE, le chevron fermant (>) a la même fonction que le crochet fermant (]). Si l'instruction d'impression d'une variable MULTILINE est fermée par un chevron fermant (>), les caractères passent à la ligne sur un espace blanc pour rester dans les limites du champ défini par le crochet ouvrant ([) et le chevron fermant (>). De même, si la variable n'est pas MULTILINE, le chevron fermant (>) permet d'afficher toutes les données sur la ligne actuelle, quelle que soit sa longueur.

- Un champ d'une instruction de mise en page peut faire référence à une variable précédemment définie ou à un nom de colonne.

- Pour faire référence à un nom de variable ou de colonne dans une autre instruction BLOCK, utilisez la syntaxe suivante :

  nom_bloc::*colonne* | *nom-variable*

Texte littéral

Le texte littéral permet d'inclure des informations supplémentaires dans votre rapport. Il s'affiche dans le rapport exactement comme spécifié dans le modèle. Pour inclure du texte littéral dans une instruction de mise en page, placez-le sur une ligne entre les accolades ouvrante ({) et fermante (}). Ne l'entourez pas de guillemets ni de crochets.

Dans cet exemple, "ACME Company" et "Page :" sont interprétés comme du texte littéral par le programme de génération de rapports de CA SDM :

```
PAGE HEADER {
                ACME Company          Page : [PG]
}
```

Informations complémentaires :

Instructions FOOTER des modèles de rapport (page 536)
Instructions PAGE FOOTER des modèles de rapport (page 539)
Instructions HEADER des modèles de rapport (page 537)
Instructions HEADER2 des modèles de rapport (page 538)
Instructions PAGE HEADER des modèles de rapport (page 539)
Instructions PRINT des modèles de rapport (page 540)

Expressions de variable dans les modèles de rapport

Chaque valeur que vous souhaitez faire apparaître dans le rapport peut être affectée à une variable. Les expressions de variable vous permettent d'effectuer les opérations suivantes :

- manipuler les données CA SDM ;
- utiliser des fonctions pour effectuer des calculs sur les valeurs extraites.

L'exemple suivant crée une variable nommée *desc* pour faire référence au contenu du champ chg_desc de la fenêtre Demande de changement. L'indicateur MULTILINE permet d'imprimer l'intégralité de la variable sur plusieurs lignes :

```
desc = description MULTILINE;
```

L'exemple suivant imprime la description. La sortie aura la longueur définie entre crochets. Si vous souhaitez faire apparaître une description plus longue, augmentez le nombre d'espaces entre les crochets.

```
PRINT { [desc  ]                                    }
```

Exemple : Modèle de rapport

Le modèle Rapport de contact affecté ci-dessous illustre la création d'un modèle de rapport. Ce modèle correspond à un rapport répertoriant les demandes de changement ouvertes auxquelles le même contact est affecté :

```
PAGE HEADER {
                                                        A partir du : [CD>
                                                               [CT>
}
PAGE FOOTER {
                          Page : [PG>
}
BLOCK chg ("SELECT \
                chg_ref_num, description, priority, \
                status, category, assignee \
      FROM Change_Request",
    "WHERE #Change_Request.status = 'OP' \
AND #Change_Request.requestor = #ca_contact.id \
AND #ca_contact.last_name = ? \
AND #ca_contact.first_name = ? \
AND #ca_contact.middle_name = ? " , $1, $2, $3)
{
        BLOCK st ("SELECT sym FROM Change_Status",
                    "WHERE code = ? ", chg::status) {}
        BLOCK (strlen(category)) cat ("SELECT sym FROM Change_Category",
                                        "WHERE code = ? ", chg::category) {}
```

```
HEADER {
                DEMANDES DE CHANGEMENT OUVERTES AYANT LE MEME DEMANDEUR / CONTACT
CHANGE ORDER Summary          Pri   Status    Category          Assignee
}
HEADER2 {
CHANGE ORDER Summary          Pri   Status    Category          Assignee
------------------------------------------------------------------------
}
        num = chg_ref_num;
        desc = description MULTILINE;
        pr = deref (priority);
        stat = st::sym;
        catgry = cat::sym;
        asgn = deref (assignee);
PRINT {
[num      ] [desc            ][pr ] [stat   ] [catgry          ] [asgn ]
}
}
```

Page Header

Indique ce qui doit être imprimé en haut de chaque page du rapport. CD et CT sont des variables prédéfinies indiquant la date et l'heure actuelles. Elles s'affichent dans l'en-tête de chaque page. Ces deux champs se terminent par un chevron de sorte que le champ puisse s'étendre jusqu'à la marge de droite. La mention « As Of: » se trouvant à l'extérieur d'un champ et sur une ligne après l'accolade ouvrante, elle s'affichera sous forme de texte littéral dans le rapport.

```
PAGE HEADER {                                   As Of:  [CD>
                                                        [CT>
}
```

Pied de page

Inclut le numéro de page avec "Page :" en tant que texte littéral.

```
PAGE FOOTER {
                                    Page : [PG>
}
```

Remarque : Les instructions PAGE HEADER et PAGE FOOTER définissant des en-têtes et des pieds de page généraux, elles ne font pas partie d'une instruction BLOCK.

Section de signalement

Crée une section de signalement pour l'instruction BLOCK principale, ainsi que pour ses instructions imbriquées. Une section de signalement fait généralement partie des données du rapport. Notez qu'ici, ce rapport ne contient qu'une section de signalement. Le nom unique de ce bloc est chg.

La clause SELECT sélectionne les colonnes à inclure dans les données du rapport à partir (FROM) de trois tables, mais uniquement lorsque les conditions spécifiées par la clause WHERE sont satisfaites.

Les trois dernières expressions AND de la clause WHERE comportent des points d'interrogation représentant des paramètres qui peuvent être remplacés et prennent les valeurs des arguments $1, $2 et $3, respectivement. Donc, $1 est pour ca_contact.last_name, $2 est pour ca_contact.first_name et $3 est pour ca_contact.middle_name. Les arguments $1, $2 et $3 obtiennent les valeurs des arguments de ligne de commande.

```
BLOCK chg (“SELECT \
...",
“WHERE \
...\
AND #ca_contact.last_name = ? \
AND #ca_contact.first_name = ? \
AND #ca_contact.middle_name = ? “, $1, $2, $3)
```

En-têtes des sections de signalement

Spécifie que l'accolade ouvrante marque le commencement de la partie programme de sortie de l'instruction BLOCK : ses instructions indiquent ce qu'il convient de faire des données extraites par les clauses SELECT et WHERE. Cet exemple comprend des instructions HEADER et HEADER2 imbriquées qui s'appliquent uniquement à cette section de signalement. L'instruction HEADER2 ne s'imprime que si le rapport couvre plusieurs pages.

```
{
   ...
   HEADER {
              DEMANDES DE CHANGEMENT OUVERTES AYANT LE MEME DEMANDEUR / CONTACT
CHANGE ORDER Summary            Pri    Status  Category  Assignee
}
   HEADER2 {
CHANGE ORDER Summary            Pri    Status  Category  Assignee
------------------------------------------------------------------------
}
```

Affectations de variables

Spécifie les expressions de variable qui agissent sur les données spécifiées par les clauses SELECT. Elles affectent des variables aux valeurs des colonnes et aux résultats des expressions. Ces variables correspondent aux champs de l'instruction PRINT ci-dessous.

Dans la variable *desc*, MULTILINE indique que les champs doivent être imprimés ou affichés sur plusieurs lignes au lieu d'être tronqués. La fonction deref permet de renvoyer l'expression de chaîne contenue dans les colonnes référencées.

```
num = chg_ref_num;
desc = description MULTILINE;
pr = deref (priority);
stat = st::sym;
catgry = cat::sym;
asgn = deref (assignee);
```

Impression

Contient les champs à imprimer. Cette instruction peut également inclure du texte littéral pour améliorer la présentation du rapport. La dernière accolade fermante correspond à l'accolade ouvrante de la section programme de sortie de l'instruction BLOCK.

```
PRINT {
[num ] [desc         ] [pr]  [stat] [catgry] [asgn         ]

}
}
```

Informations complémentaires :

Commande Report (page 526)

Génération de rapports

Une fois le modèle créé, vous pouvez générer le rapport en exécutant le programme de génération de rapports d'CA SDM. Ce programme peut être exécuté à partir de :

- la ligne de commande ;
- une option de menu d'CA SDM ;
- un fichier script.

Remarque : Si vous travaillez sur un serveur UNIX, vous pouvez inclure le paramètre de redirection de sortie de rapport (rptuiDsp) dans la commande report pour afficher une boîte de dialogue comportant des options permettant d'envoyer le rapport à l'écran, dans un fichier ou à une imprimante.

Informations complémentaires :

Affichage d'une boîte de dialogue (UNIX seulement) (page 526)

Commande Report

Pour générer un rapport à partir d'une ligne de commande, sous UNIX, utilisez la commande report de CA SDM :

`pdm_task report [-h][-e][-f][-F chaîneff][-p longueurpage] nomfichier [arguments de ligne de commande]`

Remarque : La commande report est précédée de la commande pdm_task qui définit les variables d'environnement requises. Si le rapport est conçu pour accepter des arguments de ligne de commande, vous devez en entrer une pour chaque argument dans le modèle de rapport.

Sous Windows, utilisez la commande rpt_srv :

`rpt_srv titre-rapport`

L'exemple suivant comprend les trois arguments de ligne de commande (Stévin, Jeanne et L) nécessaires pour le Rapport de contact concerné décrit précédemment dans ce chapitre dans l'exemple de modèle de rapport :

```
pdm_task report /reports/myrpt.rpt Stévin Jeanne L
```

Si un argument est vide, vous devez utiliser une chaîne NULL. Par exemple, si Jeanne Stévin n'a pas de deuxième prénom, la syntaxe est la suivante :

```
pdm_task report /reports/myrpt.rpt Stévin Jeanne ""
rpt_srv \reports\myrpt.rpt Stévin Jeanne L
```

Affichage d'une boîte de dialogue (UNIX seulement)

Vous pouvez inclure le paramètre de redirection de rapport (rptuiDsp) dans la commande report pour afficher une boîte de dialogue. Cette boîte contient des options permettant d'imprimer le rapport dans un fichier, de l'afficher dans une fenêtre Xterm ou de l'envoyer à une imprimante.

Exemple :

```
pdm_task rptuiDsp report /reports/myrpt.rpt Stévin Jeanne L
```

Cet exemple ajoute le titre "Rapport d'inventaire" à la boîte de dialogue :

```
pdm_task rptuiDsp report /reports/myrpt.rpt Stévin Jeanne L "title:Rapport
d'inventaire"
```

Référence d'un modèle de rapport

Vous pouvez utiliser des expressions, des fonctions et des instructions de variables dans un modèle de rapport.

Expressions de variable d'un modèle de rapport

Les expressions de variable définissent les données à imprimer ou à afficher dans un modèle de rapport. Elles sont placées dans une instruction de mise en page ou de bloc.

Syntaxe d'expression de variable

La syntaxe désigne les règles régissant la formation des instructions dans un langage de programmation. La structure de cette chaîne est la suivante :

nom-variable = expression [indicateurs]

Indicateurs d'expression de variable

Les indicateurs permettent de mettre en forme le résultat d'une expression de variable. Utilisez ces indicateurs pour mettre en forme les champs de texte :

MULTILINE

Affiche le texte sur plusieurs lignes au lieu de le tronquer.

RIGHT

Justifie le texte à droite.

Utilisez ces indicateurs pour mettre en forme les champs numériques :

BLANKZERO

Fonctionne comme un champ dont la valeur est nulle et qui n'imprime pas de zéro.

BOOL

Convertit la valeur zéro en non et les valeurs autres que zéro en oui.

REAL

S'affiche en tant que nombre à virgule flottante (la valeur par défaut est un nombre entier).

ZEROFILL

Affiche les zéros à gauche et à droite.

Utilisez ces indicateurs pour mettre en forme les champs de date/heure :

DATE

N'affiche que la partie date.

DAYS

Affiche les durées en jours.

HOURS

Affiche les durées en heures.

MINUTES

Affiche les durées en minutes.

SECONDS

Affiche les durées en secondes.

TIME

N'affiche que la partie heure.

Exemple d'expression de variable

La ligne suivante présente un exemple d'expression de variable :

```
desc = description MULTILINE
```

Remarques sur les expressions de variable

Les noms de variables doivent être uniques à l'intérieur d'une instruction BLOCK et ne doivent pas être identiques aux noms de colonnes dans la clause SELECT du bloc. Vous pouvez utiliser le même nom de variable dans différentes instructions BLOCK, mais vous ne pouvez pas les répéter dans une même instruction BLOCK.

Respectez les règles de syntaxe suivantes lorsque vous incluez des expressions dans votre modèle de rapport :

- Utilisez n'importe quelle expression C valide.
- N'insérez pas les noms de variables ou de colonnes entre guillemets.
- Insérez les constantes de chaîne entre guillemets simples ou doubles.
- Vous pouvez faire référence à un bloc imbriqué, mais uniquement s'il contient une seule ligne.
- Pour inclure un nom de colonne identique à un mot clé, faites-le précéder d'une barre oblique inverse (\). Par exemple, ALIAS est un mot-clé et \alias un nom de colonne.
- Utilisez le signe dollar ($) pour référencer les variables d'environnement telles que $name, ainsi que les arguments de ligne de commande tels que $*n*, *n* correspondant à la position de l'argument sur la ligne de commande.

- Pour préciser le nombre d'arguments de ligne de commande, utilisez $#. Par exemple, l'expression suivante signifie que si le nombre d'arguments de ligne de commande est supérieur à un, il faut utiliser l'argument supplémentaire comme un argument ; sinon, vous devez définir sa valeur comme une chaîne vide. Le modèle de rapport lui-même est considéré comme un argument de ligne de commande. Le nombre d'arguments est donc toujours au moins un.

  ```
  $# > 1 ? $1 : "
  ```

- Utilisez ## pour concaténer deux chaînes, par exemple :

  ```
  title = "Il s'agit de " ## "la première ligne. "

  long_name = fn

  irst_name ## last_name
  ```

- Les types suivants sont pris en charge :
  - (number)
  - (string)
  - (date_time)
  - (duration)
- Pour référencer un nom de variable ou de colonne dans un autre bloc, faites-le précéder de son nom de bloc suivi de deux fois deux-points, Par exemple :

  nom_bloc::*colonne* | *nom-variable*

Fonctions d'un modèle de rapport

Vous pouvez utiliser les fonctions suivantes dans votre modèle de rapport :

is_null (*expr*)

Cette fonction renvoie true (vrai) si l'expression est null.

```
false = 0

true = is_null (false)
```

sqrt (*expr*)

Cette fonction calcule la racine carrée de l'expression.

```
nine = 9

three = sqrt (nine)
```

pow (*expr1, expr2*)

Cette fonction élève *expr1* à la puissance *expr2.*

```
two = 2

three = 3

eight = pow (two,three)
```

log (*expr, expr*)

Cette fonction calcule le logarithme naturel de l'expression.

```
ten = 10

result = log (ten)
```

catname (*expr*, *expr*, *expr*)

Cette fonction concatène trois chaînes représentant un nom de contact dans une chaîne séparée par des virgules, conformément aux règles figurant dans le fichier de format des champs.

```
last = "Martinez"

first = "Franck"

middle = "P"

contact_name=catname (last, first, middle)
```

strlen (*chaîne*)

Cette fonction renvoie la longueur de la chaîne.

```
buffer = "Chaîne de 30 caractères"

thirty = strlen(buffer)
```

strindex *(chaîne, modèle [, start_index]*)

Cette fonction renvoie l'index de la première concordance de modèle ou de la concordance suivante après start_index, dans la chaîne. Renvoie -1 s'il n'existe aucune concordance.

```
buffer = "Chaîne de 30 caractères"

zero = strindex(buffer, " [A-Z] ")

two = strindex(buffer, " [a-z] ")
```

substr (*chaîne, modèle [, longueur]*)

Cette fonction renvoie la partie de la chaîne après la première concordance de modèle. Sa longueur est définie et limite la longueur de la chaîne en sortie. Renvoie une chaîne de longueur zéro s'il n'existe aucune concordance.

```
buffer = "Chaîne de 30 caractères"

last_word = substr(buffer, " [a-z]*$ ")

first_capital_letter = substr(buffer, " [A-Z] ",
    1)
```

substr *(chaîne, index [, longueur]*)

Cette fonction renvoie la portion de la chaîne située après l'index. Sa longueur est définie et limite la longueur de la chaîne de sortie. Renvoie une chaîne de longueur zéro s'il n'existe aucune concordance.

```
buffer = "Résumé : La carte réseau affiche un
    code de ... "

summary = substr(buffer, 9)

30_char_summary = strindex(buffer, 9, 30)
```

Les fonctions restantes (pseudo-fonctions) s'effectuent sur un bloc de données plutôt que sur des expressions de variable. Ces fonctions sont généralement placées dans une instruction BLOCK pour obtenir des informations sur les données d'une instruction BLOCK imbriquée.

count (*nom-bloc*)

Renvoie le nombre de lignes dans le bloc spécifié dans l'instruction BLOCK. Le nom du bloc doit être une chaîne simple.

```
Exemple de BLOCK ("SELECT id FROM Contact") {

entries = count (sample)

}
```

sum (*nom-bloc, expr*)

Exécute l'expression pour chaque ligne du bloc spécifié et totalise le résultat.

```
BLOCK sample ("SELECT actual_cost, est_cost FROM Change_Request") {

difference = sum (sample, est_cost-actual_cost)

}
```

average (*nom-bloc*, *expr*)

Exécute l'expression pour chaque ligne du bloc et renvoie la moyenne du résultat.

```
BLOCK sample ("SELECT actual_cost, est_cost FROM Change_Request"){

avg_difference = average (sample, est_cost-actual_cost)

}
```

prev (*expr*)

Renvoie la valeur précédente de l'expression. Cette fonction doit être utilisée avec précaution pour éviter d'écraser accidentellement la dernière valeur.

downtime *(planification_sla, expr1, expr2 [, bloc-délai, expr, expr]*)

Appelle un calcul du temps d'arrêt du SLA. Le premier argument doit être une chaîne identifiant un horaire. Les autres arguments correspondent aux heures de début et de fin :

expr1 correspond à la date/heure de début de l'événement.

expr2 correspond à la date/heure de fin de l'événement.

Dans cet exemple, l'instruction BLOC wrkshft extrait le planning de travail, l'instruction BLOC evt_dly extrait les délais, et la fonction downtime utilise ces enregistrements pour calculer le temps d'arrêt.

BLOCk attevt ("SELECT start_time, fire_time, event_tmpl, obj_id FROM Attached_Events")

```
{
BLOCK evt ("SELECT persid, sym, work_shift FROM Events ", "WHERE persid = ?",
attevt::event_tmpl) {}
BLOCK wrkshft ("SELECT sched FROM Bop_Workshift", "WHERE persid = ?",
evt::work_shift) {}

BLOCK evt_dly ("SELECT start_time, stop_time FROM Event_Delay", "WHERE obj_id =
?", attevt::obj_id) {}
total_downtime = downtime(wrkshft::sched,
attevt::start_time,  attevt::fire_time,
evt_dly,
evt_dly::start_time, evt_dly::stop_time);
}
```

deref (*nom-colonne*)

Renvoie la représentation du pointeur sous forme de chaîne en effectuant une recherche automatique dans la table appropriée.

```
BLOCK chg ("SELECT organization FROM Change_Request") {

org = deref (organization)

}
```

Cette pseudo-fonction impliquant des recherches, elle n'est valide que si elle est le seul élément dans l'expression. L'exemple suivant est correct :

```
model = deref (nr_model)
```

L'exemple suivant est incorrect :

```
model = "model"  ## deref (nr_model)
```

Remarque : Les références anticipées à des variables ou blocs sont interdites.

Instructions BLOC des modèles de rapport

Instructions de bloc pour définir les tables de la base de données dans lesquelles les données seront extraites et peut inclure les actions à effectuer sur ces données.

Syntaxe d'instruction de bloc

La syntaxe désigne les règles régissant la formation des instructions dans un langage de programmation. La structure de cette chaîne pour BLOCK est la suivante :

```
BLOCK nom_bloc (
       "SELECT [ALIAS,] nom_champ[, nom_champ ...]
       FROM nom_table[, nom_table ...] "
       [,"WHERE clause_where"][, arguments,] )
       [SORT "clause sort"]
{
Instructions du programme de sortie
}
```

Paramètres d'instruction de bloc

nombloc

Identifie le bloc. Chaque *nom de bloc* doit être unique.

Clause SELECT

La clause SELECT suit le *nom de bloc* et est délimitée par des guillemets doubles. Cette clause permet de répertorier les colonnes à extraire, suivies du mot-clé FROM, puis des tables dans lesquelles elles doivent être extraites. La clause SELECT est obligatoire. Voici un exemple dans lequel trois tables sont spécifiées :

```
“SELECT open_date, chg_ref_num \

last_name, first_name \

FROM Change_Request, \

ca_contact”
```

Vous ne pouvez pas inclure de pseudonyme (alias) SQL, tel que :

```
"SELECT open_date As OpenDate"
```

clause WHERE

(Facultatif) Suit la clause SELECT et qualifie plus en détail l'information sélectionnée. Elle peut être une constante de chaîne ou une expression correspondant à une chaîne. Si la clause WHERE est une chaîne vide, tous les enregistrements sont renvoyés. Les clauses WHERE peuvent contenir des arguments de remplacement (faisant référence à des variables ou à des arguments de ligne de commande). Pour cela, utilisez le point d'interrogation (?). La clause WHERE suivante pourrait suivre la clause SELECT précédente :

```
“WHERE #Change_Request.open_date >= ? \

AND #Change_Request.active_flag = 1 \

AND #ca_contact.last_name = ? ", $1
```

Remarque : La clause WHERE doit être distincte de la clause SELECT, car la première peut correspondre à une expression qui évalue une chaîne, alors que la dernière correspond toujours à une constante de chaîne. Vous disposez ainsi d'une plus grande souplesse et d'un plus grand nombre de possibilités pour manipuler des données lors de la création de votre rapport.

Clause SORT

(Facultatif) Peut suivre les clauses SELECT et WHERE. Cette clause permet de trier les lignes de données extraites. La clause SORT se présente comme la clause SQL ORDER BY. Voici un exemple :

```
SORT "open_date"
```

Instructions du programme de sortie

Elles contrôlent l'exécution du rapport. Dans un premier temps, si l'instruction HEADER est incluse, elle imprime le texte de l'en-tête du bloc. La requête de données est ensuite exécutée. Si des données sont renvoyées, chaque instruction est exécutée dans l'ordre de rédaction, à une exception près. Les fonctions de bloc, telles que sum et average, se comportent comme si elles se trouvaient à la fin du programme de sortie. En effet, leurs valeurs ne sont stables que lorsque l'exécution passe à l'enregistrement de données suivant.

Important : Le programme de sortie dépend de la réussite de la requête de données. Si aucune donnée n'est renvoyée, le programme de sortie ne s'exécute pas, à l'exception de l'instruction HEADER.

Exemple d'instruction Block

Cette instruction BLOCK suppose qu'un argument transmis contiendra un nombre entier égal à la priorité de la demande de changement. La clause WHERE vérifie d'abord le nombre d'arguments transmis ($#). S'il y en a un, il sert à évaluer l'expression pour produire la clause WHERE ; sinon on utilise une clause WHERE NULL (" ").

```
BLOCK chg ("SELECT priority FROM Change_Request",
$# > 1 ? "WHERE priority =" ## $1 :  "") {
```

Exemple d'instruction Footer

Les lignes suivantes présentent un exemple d'instruction Footer :

```
FOOTER {
     Informations récapitulatives :
             Total d'échecs : [Fail_count >
             Total de temps d'arrêt : [Downtime >
}
```

Remarques sur les instructions Block

Vous pouvez placer les instructions HEADER, HEADER2, FOOTER et PRINT, ainsi que des expressions de variable entre des accolades. Toutes les instructions seront exécutées pour chaque ligne sélectionnée.

Remarque : Les instructions PAGE HEADER et PAGE FOOTER ne peuvent pas être placées dans une instruction BLOCK.

Instructions FOOTER des modèles de rapport

Cette instruction place des informations en bas de chaque section de signalement.

Syntaxe d'instruction Footer

La syntaxe désigne les règles régissant la formation des instructions dans un langage de programmation. La structure de cette chaîne pour FOOTER est la suivante :

F0OTER *{paramètres}*

Paramètres d'instruction Footer

Les paramètres sont les suivants :

CD

Variable prédéfinie utilisée pour afficher la date actuelle.

CT

Variable prédéfinie utilisée pour afficher l'heure actuelle.

PG

Variable prédéfinie utilisée pour afficher le numéro de page actuel.

colonne | nom-variable

Ce champ peut correspondre à une variable provenant d'une expression précédente ou à une référence à une colonne dans la clause SQL d'une instruction BLOC.

texte-littéral

Tout texte autre qu'une variable prédéfinie ou qu'un nom de colonne ou de variable est interprété comme du texte littéral. Le texte littéral inclus dans l'instruction FOOTER apparaît à la position horizontale exacte à laquelle vous l'avez entré.

Remarques sur les instructions Footer

Les instructions FOOTER sont imprimées en bas de chaque section de signalement. Elles sont généralement utilisées pour présenter des résumés ou des statistiques. Vous pouvez inclure une instruction FOOTER dans une instruction BLOCK.

Le contenu d'un champ occupe l'espace exact délimité par les crochets. Les caractères en trop sont tronqués. Cependant, vous pouvez fermer un champ avec un chevron fermant (>) pour que son contenu s'étende jusqu'à la marge de droite.

Pour faire référence à un nom de variable ou de colonne dans une autre instruction BLOCK, utilisez la syntaxe suivante :

nom_bloc::*colonne* | *nom-variable*

Instructions HEADER des modèles de rapport

Cette instruction place des informations en haut de chaque section de signalement.

Syntaxe d'instruction Header

La syntaxe désigne les règles régissant la formation des instructions dans un langage de programmation. La structure de cette chaîne pour HEADER est la suivante :

HEADER {*paramètres*}

Paramètres d'instruction Header

Pour obtenir une liste des paramètres valides pour cette instruction, ainsi que leur description, consultez la section Instructions HEADER des modèles de rapport (page 539).

Exemple d'instruction Header

Les lignes suivantes présentent un exemple d'instruction Header :

```
HEADER {
                Rapport résumé du contact
     Nom Contact Alias Contact Organisation
}
```

Remarques sur les instructions Header

Les instructions HEADERS sont imprimées au début de chaque section de signalement et peuvent être incluses dans une instruction BLOCK. Les instructions HEADERS sont généralement utilisées pour présenter des titres de colonne et/ou de section.

Le contenu d'un champ occupe l'espace exact délimité par les crochets. Les caractères en trop sont tronqués. Cependant, vous pouvez fermer un champ avec un chevron fermant (>) pour que son contenu s'étende jusqu'à la marge de droite.

Remarque : Si l'instruction d'impression d'une variable MULTILINE est fermée par un chevron fermant (>), les caractères passent à la ligne sur un espace blanc pour rester dans les limites du champ défini par le crochet ouvrant ([) et le chevron fermant (>). De même, si la variable n'est pas MULTILINE, le chevron fermant (>) permet d'afficher toutes les données sur la ligne actuelle, quelle que soit sa longueur.

Pour faire référence à un nom de variable ou de colonne dans une autre instruction BLOCK, utilisez la syntaxe suivante :

nom_bloc::*colonne* | *nom-variable*

Instructions HEADER2 des modèles de rapport

Cette instruction place la suite des informations d'en-tête en haut de chaque page d'une section de signalement si cette section couvre plusieurs pages.

Syntaxe d'instruction Header2

La syntaxe désigne les règles régissant la formation des instructions dans un langage de programmation. La structure de cette chaîne pour HEADER2 est la suivante :

HEADER2 {*paramètres*}

Paramètres d'instruction Header2

Pour obtenir une liste des paramètres valides pour cette instruction, ainsi que leur description, consultez la section Instructions HEADER2 des modèles de rapport (page 538).

Exemple d'instruction Header2

```
HEADER2 {
   Rapport résumé du contact (suite)
   Nom Contact Alias Contact Organisation
}
```

Remarques sur les instructions Header2

Une instruction HEADER2 peut être incluse dans une instruction BLOCK.

Le contenu d'un champ occupe l'espace exact délimité par les crochets. Les caractères en trop sont tronqués. Cependant, vous pouvez fermer un champ avec un chevron fermant (>) pour que son contenu s'étende jusqu'à la marge de droite.

Pour faire référence à un nom de variable ou de colonne dans une autre instruction BLOCK, utilisez la syntaxe suivante :

nom_bloc::*colonne* | *nom-variable*

Instructions PAGE FOOTER des modèles de rapport

Cette instruction place des informations en bas de chaque page du rapport.

Syntaxe d'instruction Page Footer

```
PAGE FOOTER {paramètres}
```

Paramètres d'instruction Page Footer

En dehors du fait que vous ne pouvez pas utiliser de noms de colonnes et de variables, les paramètres de cette instruction sont les mêmes que ceux de l'instruction FOOTER. Pour obtenir une liste des paramètres valides pour cette instruction, ainsi que leur description, consultez la section Instructions PAGE FOOTER des modèles de rapport (page 539).

Paramètres d'un exemple d'instruction Page Footer

```
PAGE FOOTER {
                Numéro de page : [PG>
}
```

Remarques sur les paramètres d'exemple d'instruction Page Footer

Le contenu d'un champ occupe l'espace exact délimité par les crochets. Les caractères en trop sont tronqués. Cependant, vous pouvez fermer un champ avec un chevron fermant (>) pour que son contenu s'étende jusqu'à la marge de droite.

Pour faire référence à un nom de variable ou de colonne dans une autre instruction BLOCK, utilisez la syntaxe suivante :

nom_bloc::*colonne* | *nom-variable*

Instructions PAGE HEADER des modèles de rapport

Cette instruction place des informations en haut de chaque page du rapport.

Syntaxe d'instruction Page Header

La syntaxe désigne les règles régissant la formation des instructions dans un langage de programmation. La structure de cette chaîne pour PAGE HEADER est la suivante :

```
PAGE HEADER {paramètres}
```

Paramètres d'instruction Page Header

En dehors du fait que vous ne pouvez pas utiliser de noms de colonnes et de variables, les paramètres de cette instruction sont les mêmes que ceux de l'instruction FOOTER. Pour obtenir une liste des paramètres valides pour cette instruction, ainsi que leur description, consultez la section Instructions PAGE FOOTER des modèles de rapport (page 539).

Exemple d'instruction Page Header

```
PAGE HEADER {
   Date of Report:  [CD>
   Time of Report:  [CT>
}
```

Remarques d'instruction Page Header

Les instructions PAGE HEADERS sont imprimées en haut de chaque page du rapport. Elles peuvent être définies à n'importe quel emplacement du modèle de rapport, mais elles ne doivent pas être incluses dans une instruction BLOCK.

Le contenu d'un champ occupe l'espace exact délimité par les crochets. Les caractères en trop sont tronqués. Cependant, vous pouvez fermer un champ avec un chevron fermant (>) pour que son contenu s'étende jusqu'à la marge de droite.

Pour faire référence à un nom de variable ou de colonne dans une autre instruction BLOCK, utilisez la syntaxe suivante :

nom_bloc::*colonne* | *nom-variable*

Instructions PRINT des modèles de rapport

Cette instruction place des données dans une section de signalement.

Syntaxe d'instruction Print

La syntaxe désigne les règles régissant la formation des instructions dans un langage de programmation. La structure de cette chaîne pour PRINT est la suivante :

```
PRINT {paramètres}
```

Paramètres d'instruction Print

Reportez-vous à la section FOOTER (page 536) pour obtenir la liste des paramètres valides pour cette instruction, ainsi que leur description.

Exemple d'instruction Print

```
PRINT {
[num ] [desc          ] [pr]  [stat] [catgry] [asgn              ]
}
```

Remarques sur les instructions Print

Placez l'instruction PRINT à l'endroit où vous souhaitez que les données d'une section de signalement apparaissent dans le rapport. Vous pouvez inclure une instruction PRINT dans une instruction BLOCK.

Le contenu d'un champ occupe l'espace exact délimité par les crochets. Les caractères en trop sont tronqués. Cependant, vous pouvez fermer un champ avec un chevron fermant (>) pour que son contenu s'étende jusqu'à la marge de droite.

Remarque : Si l'instruction d'impression d'une variable MULTILINE est fermée par un chevron fermant (>), les caractères passent à la ligne sur un espace blanc pour rester dans les limites du champ défini par le crochet ouvrant ([) et le chevron fermant (>). De même, si la variable n'est pas MULTILINE, le chevron fermant (>) permet d'afficher toutes les données sur la ligne actuelle, quelle que soit sa longueur.

Pour faire référence à un nom de variable ou de colonne dans une autre instruction BLOCK, utilisez la syntaxe suivante :

nom_bloc::*colonne* | *nom-variable*

Personnalisation des rapports Crystal

L'affichage de ces rapports est soumis aux conditions suivantes :

- Vous devez copier les rapports Crystal disponibles dans le répertoire Crystal $NX_ROOT/bopcfg/rpt pour qu'ils soient accessibles à partir du sélecteur de rapports Crystal.
- Votre client de base de données doit fonctionner, être en cours d'exécution et disposer d'une connexion établie vers le serveur de base de données s'exécutant soit sur le même ordinateur, soit sur un ordinateur différent. Si vous utilisez un client CA SDM pour exécuter vos rapports Crystal ou Access, vous devez au préalable installer un client de base de données pour la base de données spécifique et établir une connexion au serveur de la base de données pour pouvoir exécuter ces rapports.

Une fois que vous avez créé des rapports Crystal personnalisés, procédez comme suit :

1. Copiez les rapports Crystal personnalisés dans le répertoire Crystal suivant :

   ```
   $NX_ROOT/bopcfg/rpt
   ```

2. Ajoutez les noms de fichiers des rapports Crystal personnalisés dans le fichier de configuration suivant :

   ```
   crystal.cfg
   ```

Vous pouvez ensuite accéder aux rapports Crystal. Pour ce faire, cliquez sur le menu Démarrer dans la barre des tâches, puis choisissez Signalement, Service Desk Reporting (Crystal Reports) dans le menu CA SDM (accessible à partir du menu Programmes). La fenêtre Service Desk Reporting (Crystal) s'affiche.

Important : Les clients CA SDM ne peuvent pas faire l'objet d'une mise à niveau. Par conséquent, si vous créez et utilisez des rapports Crystal sur le serveur CA SDM et que vous prévoyez de mettre à niveau votre version de CA SDM, vous devez copier tous les rapports personnalisés dans un autre emplacement pour ne pas les perdre. Après la mise à niveau, copiez de nouveau les rapports dans le répertoire $NX_ROOT/bopcfg/rpt Crystal, puis modifiez le fichier crystal.config pour que les rapports soient accessibles à partir du sélecteur de rapports.

Chapitre 10: Remplissage de CA CMDB

Ce chapitre traite des sujets suivants :

Remplissage de la base de données (page 543)
Remplissage du chargeur général de ressources de la base de données (GRLoader) (page 543)
Utilisation du chargeur général de ressources pour importer des données (page 544)
Affectations de classe et de famille (page 544)
Chargement de données CA APM (page 545)

Remplissage de la base de données

L'insertion dans CMDB des éléments de configuration de votre infrastructure informatique et de leurs relations entre eux, fait partie intégrante de l'utilisation efficace de cette application. Vous pouvez remplir CMDB manuellement, au moyen de l'éditeur d'éléments de configuration intégré, ou en important des éléments provenant d'autres outils de gestion d'actifs.

Remarque : Pour plus d'informations sur l'éditeur d'éléments de configuration, reportez-vous à *l'Aide en ligne*.

Remplissage du chargeur général de ressources de la base de données (GRLoader)

Pour remplir la base de données en chargeant des éléments de configuration et des relations, effectuez les tâches suivantes :

1. Convertissez les données d'entrée contenant des informations concernant des éléments de configuration et leurs relations en XML ou dans une feuille de calcul.
2. Le programme du chargeur général de ressources de CA CMDB utilise les données XML comme entrées.
3. Le chargeur général de ressources charge les données dans la base de données.

   Remarque : Pour plus d'informations sur les paramètres du chargeur général de ressources, reportez-vous au *Manuel de référence technique de CA CMDB*.

Informations complémentaires :

Utilisation du chargeur général de ressources pour importer des données (page 544)

Utilisation du chargeur général de ressources pour importer des données

Importez les données à l'aide du chargeur général de ressources fourni avec CA SDM, qui crée des éléments de configuration en fonction des données dans un fichier XML ou une feuille de calcul Excel.

1. Dans le menu Démarrer, cliquez sur Exécuter.
2. Entrez **cmd**.

   Une fenêtre de commande DOS s'affiche.
3. Entrez la commande suivante :

   `Grloader -u <nom d'utilisateur> -p <mot de passe> -s http://<nom serveur_ca_sdm>:8080 -i <document_xml ou feuille de calcul>`

   Le chargeur général de ressources crée des CI à partir des données contenues dans le fichier XML. Si des erreurs surviennent au cours de ce processus, un fichier d'erreurs est créé qui répertorie les CI n'ayant pas pu être importés et pour quelle raison.

   L'importation du chargeur général de ressources est terminée.
4. Démarrez CA SDM et vérifiez que les données de CI ont été correctement remplies.
5. Démarrez le visualiseur CMDB pour vérifier que les données de relation ont été correctement remplies.

   Les données sont importées et vérifiées.

   Remarque : Pour plus d'informations sur le chargeur général de ressources, reportez-vous au *Manuel de référence technique de CA CMDB*.

Affectations de classe et de famille

Appliquez un schéma de classification à chaque CI ; ce schéma implique d'affecter les attributs suivants à chaque Ci :

- Famille : une collection d'éléments de configuration ayant des attributs similaires
- Classe : un sous-ensemble d'éléments de configuration dans une famille

Vous pouvez créer des affectations comme suit.

- Renseignez les données du fabricant qui identifient la famille et la classe pour chaque actif matériel.
- Insérez des valeurs non vides de famille et de classe dans les colonnes correspondantes du fichier d'entrée.

Le chargeur général de ressources n'importe pas les CI dont la famille et la classe ne font pas partie des familles et classes existantes.

Chargement de données CA APM

Les entrées principales au programme de chargeur CA Asset Portfolio Management (CA APM) sont une table ou un affichage qui contient un extrait des données CA APM. Ces données sont contenues dans la table ou vue de base de données CMDB_Export_Asset_Data. Dans certains cas, les données à importer dans la MDB sont situées dans la même base de données que la cible. Toutefois, dans de nombreuses circonstances, les données d'importation se trouvent dans une base de données différente, par exemple lors d'une importation de données provenant d'une autre filiale. Dans les deux cas, créez une vue dans la base de données qui contient les données source.

La vue des données CA APM ne contient pas les attributs de classe et de famille et elle provient peut-être d'un système qui n'utilise pas le même schéma de classification. Par exemple, si les données d'actifs proviennent d'une autre entreprise, un système de classification différent peut être utilisé.

La table CA_MODEL_DEF contient une liste de modèles ; chaque modèle est recherché dans les données de CMDB_Export_Asset_Data. S'il s'y trouve, la famille et la classe de ce modèle sont affectées à l'actif en cours d'importation. S'il en est absent, définissez un nouveau modèle pour l'actif. Vous pouvez copier des entrées de la table CA_MODEL_DEF source dans la MDB cible ou insérer dans la table CA_MODEL_DEF des entrées pour toutes les nouvelles marques de matériel et tous les nouveaux numéros de modèles.

Chapitre 11: Utilisation du lanceur RDG (référentiel de données de gestion)

Ce chapitre explique comment définir des RDG, importer des données, mapper des CI à leur source et afficher des données fédérées pour un CI.

Ce chapitre traite des sujets suivants :

Lanceur RDG (page 547)
Terminologie RDG (page 548)
Mappage RDG (page 549)
Lancement RDG (page 550)
Visionneuse CMDBf (page 550)
Définition d'un RDG dans CA CMDB (page 550)
Federation et le chargeur général de ressources (page 559)
Mappage des CI RDG et des CI CA CMDB (page 561)
Configuration des RDG pour la visionneuse CMDBf (page 563)
Lancement de l'interface de navigateur Web RDG (page 563)
Intégration CA Cohesion (page 564)

Lanceur RDG

Le regroupement de données provenant de plusieurs sources (appelées RDG) constitue l'un des objectifs principaux de la mise en oeuvre de CA CMDB. Toutefois, un CI doit toujours comporter une référence à son RDG d'origine.

CA CMDB permet d'importer et de charger des CI, mais aussi d'associer les CI à leur origine. En outre, vous pouvez utiliser le lanceur RDG lorsque vous affichez un CI dans CA CMDB pour accéder en toute transparence au système d'où provient le CI, comme illustré par le diagramme ci-dessous.



Au moyen du lanceur RDG, vous pouvez mettre en oeuvre une procédure de gestion des changements en "boucle fermée" comme suit.

1. Créez un enregistrement de changement.
2. Mettez en oeuvre le changement.
3. Contrôlez le changement en vérifiant la source RDG.
4. Mettez à jour CMDB pour indiquer que le changement a été effectué.

Dans le cadre d'une procédure de gestion des problèmes, vous pouvez utiliser le lanceur RDG comme suit.

1. Détectez un problème.
2. Déterminez la gravité et l'omniprésence du problème à l'aide des données de relations entre CI qui peuvent indiquer les CI de dépendants affectés.
3. Déterminez les causes possibles du problème en recherchant les CI de fournisseurs.
4. Effectuez une analyse en profondeur, si nécessaire, au moyen des informations extrêmement détaillées disponibles dans le RDG et utilisez celui-ci pour entreprendre des actions correctives.

Terminologie RDG

Les termes suivants sont utilisés dans l'intégration CMDB-RDG.

Un RDG (référentiel de données de gestion) représente des logiciels ou des données qui contiennent des informations sur la source d'un CI. En général, un RDG contient davantage d'informations non affinées sur les CI que CMDB, qui contient un sous-ensemble géré de ces données.

Une *classe de RDG* (MDR_CLASS) est utilisée pour regrouper les RDG traités de façon similaire par CA CMDB. Il y a trois classes RDG spéciales : **COHESION**, **GLOBAL** et **cmdbf**.

Un *nom de RDG* (MDR_NAME) est le nom utilisé par un RDG pour faire référence à lui-même. Vérifiez que la combinaison des valeurs mdr_name et mdr_class soit unique au sein de votre entreprise.

Un ID d'actif fédéré (FEDERATED_ASSET_ID) est l'identificateur RDG unique pour un CI.

En général, différentes familles de CI utilisent respectivement différents RDG comme fournisseurs de données. Toutefois, un seul CI peut disposer de plusieurs fournisseurs de données RDG. Par exemple :

Famille de CI	MDR_CLASS
Contact	système de ressources humaines annuaire téléphonique système d'authentification unique
Document	système de gestion de documents
Climatisation	système de gestion de documents système de gestion de contrats système de contrôle de la climatisation

Famille de CI	MDR_CLASS
Ordinateur central	système de gestion de bandes système de gestion DASD système de gestion des performances planificateur d'opérations
Stockage	système de gestion du stockage système de gestion des actifs
Emplacement	système de gestion des actifs calendrier de formation répertoire du bureau
Réseau	systèmes de gestion de réseau système de gestion des problèmes

Chaque classe RDG peut comporter plusieurs RDG et chaque RDG peut fournir des données à plusieurs CI. Un CI peut recevoir des données provenant de zéro, un ou plusieurs RDG. Un CI peut également recevoir des données de façon indépendante. Par exemple, un CI d'ordinateur central peut comporter des données fournies par le système de gestion de disques 1, alors qu'un autre CI 'ordinateur central peut comporter des données fournies par le système de gestion de disques 2 et le planificateur d'opérations 2. CA CMDB gère les relations entres les CI et leurs RDG associés.

Mappage RDG

Chaque RDG dispose d'un moyen unique d'identifier les CI qu'il gère. Ces identificateurs sont rarement synchronisés d'un RDG à l'autre. Par exemple, pour référencer un CI Contact donné, différents RDG peuvent utiliser un numéro de sécurité sociale, un numéro de téléphone, un numéro de permis de conduire ou un ID d'employé pour désigner la même personne. Le processus d'association de ces identificateurs disparates à un même identificateur unique (UUID), géré par la MDB, est appelé *mappage*. Le mappage a lieu automatiquement lorsque des données sont importées au moyen du chargeur général de ressources si le CI contient les balises <mdr_name> <mdr_class> et <federated_asset_id>. Un mappage manuel est également possible au moyen des fonctions d'administration de l'interface utilisateur. Un CI qui n'est associé à aucun mappage est appelé un CI *non fédéré*. Chaque CI est mappé automatiquement à des RDG globaux en utilisant l'UUID comme ID actif fédéré.

Lancement RDG

Lorsque vous affichez un CI en utilisant l'interface utilisateur de CA CMDB, vous pouvez cliquer sur une série de boutons pour directement lancer une interface utilisateur du RDG. Il y a un bouton par mappage RDG pour le CI central. Cela est particulièrement utile lorsque vous souhaitez vérifier qu'une demande de changement s'est terminée avec succès ou pour obtenir des informations supplémentaires sur un CI lorsque les données ne sont pas collectées par CMDB.

Visionneuse CMDBf

CA SDM permet à la visionneuse CMDBf d'afficher les résultats de la fédération des CI d'un RDG à l'autre. A partir d'une page de détails des CI (ou à partir du menu contextuel des CI sur la liste des CI), cliquez sur Visionneuse CMDBf pour afficher les attributs de CI des CMDB et des RDG fédérés en parallèle. Sur la page de vue fédérée, vous pouvez cliquer sur Récupérer pour mettre à jour les informations à partir de l'un des RDG fédérés. Pour une meilleure lisibilité, les fichiers de métadonnées de CA CMDB peuvent rapprocher les noms d'attribut de RDG et les noms d'attribut de CA CMDB.

Remarque : Cette fonctionnalité nécessite que les RDG prennent en charge les requêtes. Configurez les terminaux CMDBf des RDG pour afficher leurs résultats dans la vue fédérée. Pour plus d'informations, consultez le *Manuel de mise en oeuvre*.

Définition d'un RDG dans CA CMDB

Avant d'utiliser la visionneuse CMDBf, vous devez définir le RDG sur CA CMDB.

Pour définir un nouveau RDG sur CA CMDB :

1. Sur l'onglet d'Administration, accédez à CA CMDB, Gestion RDG, Liste des RDG.
2. Cliquez sur Créer.

   La page Créer une définition RDG apparaît.
3. Remplissez les champs suivants :

   Client hébergé

   Identifie le propriétaire du client hébergé de ce RDG (si l'hébergement multiclient est installé).

   Nom du bouton

   Spécifie l'étiquette de bouton RDG qui doit s'afficher sur la page Détails du CI. Ce nom doit être unique pour chaque RDG. Obligatoire pour le lancement en fonction du contexte et la visionneuse CMDBf.

Nom du RDG

Spécifie la chaîne à faire correspondre aux données XML qui est envoyée dans le champ mdr_name. Bien que le RDG puisse utiliser n'importe quelle chaîne, il utilise souvent le nom d'hôte. Ce nom, associé à mdr_class, forme un nom unique pour le RDG. Obligatoire pour le lancement en fonction du contexte et la visionneuse CMDBf.

Classe RDG

Spécifie la classe devant correspondre aux données envoyées dans le champ mdr_class du fichier XML. Bien que ce nom soit libre il doit, associé au champ mdr_name, former un identificateur unique pour le RDG. Les RDG globaux sont définis avec une classe RDG GLOBAL.

- Les RDG CA Cohesion ACM doivent spécifier une classe RDG COHESION qui définit automatiquement les champs Chemin, Paramètres et URL à lancer sur les valeurs de lancement dans le contexte CA Cohesion ACM requises.
- Les RDG CA Asset Portfolio Management r11.3.4 doivent spécifier un nom RDG APM et une classe RDG GLOBAL qui définit automatiquement les champs Chemin, et de Paramètres et URL à lancer sur les valeurs de lancement dans le contexte CA Asset Portfolio Management r11.3.4 requis.
- Les RDG CA APM r12.5 doivent spécifier un nom RDG ITAM et une classe RDG GLOBAL, qui définit les champs Chemin, Paramètres et URL à lancer sur les valeurs de lancement dans le contexte CA APM 12.5 requis.
- Pour la visionneuse CMDBf, la classe du RDG doit être cmdbf.

Actif

Indique cette définition du RDG comme activée ou désactivée. Les définitions du RDG désactivées sont supprimées logiquement, mais elles peuvent être réactivées à l'aide de l'utilitaire Recherche.

Propriétaire

Spécifie le contact responsable de ce RDG.

description

Spécifie une description en texte au format libre.

Nom d'hôte

Spécifie le nom d'hôte, le nom DNS ou l'adresse IP de l'hôte, qui contient le serveur Web qui héberge la page Web à lancer. Obligatoire pour le lancement en fonction du contexte.

Port

Spécifie le port TCP/IP utilisé par le serveur Web du RDG pour afficher les pages Web. Le port par défaut est 80. Obligatoire pour le lancement en fonction du contexte.

chemin

Spécifie la portion de l'URL qui précède le point d'interrogation (?). Cette information se trouve dans la documentation liée au RDG.

- Pour la mdr_class Cohesion, la valeur est automatiquement définie sur "CAisd/html/cmdb_cohesion.html" et ne peut être modifiée.
- Pour mdr_name APM et mdr_class GLOBAL, la valeur est définie automatiquement sur apm/frmObject.aspx et elle ne peut pas être modifiée.
- Pour mdr_name ITAM et mdr_class GLOBAL, la valeur est définie automatiquement sur ITAM/Pages/Asset.aspx et elle ne peut pas être modifiée.

Paramètres

Spécifie la portion de l'URL qui suit le point d'interrogation (?). Cette information se trouve dans la documentation liée au RDG.

- Pour la mdr_class Cohesion, cette valeur est automatiquement définie sur "hostname={nom_hôte}+port={port}+family={famille}+name={nom}+secret={mot_de_passe}+federated_asset_id={id_actif_fédéré}" et ne peut être modifiée.
- Pour mdr_name UAPM et mdr_class GLOBAL, la valeur est définie automatiquement sur ObjectID={ID_actif_cmdb}&obj=11&FUNCTION=1&WinID=OBFRASSET{ID_actif_cmdb}&WinContainerID= et elle ne peut pas être modifiée.
- Pour mdr_name ITAM et mdr_class GLOBAL, la valeur est définie automatiquement sur ParentClass=Asset&assetid={cmdb_asset_id}&TicketID={itam_ticketid} et elle ne peut pas être modifiée.

ID d'utilisateur

Spécifie l'ID de connexion au RDG, s'il est requis. Cette valeur remplace {id_utilisateur} dans l'URL. Si cette valeur est laissée vide, l'ID de l'utilisateur prend par défaut la valeur de l'ID de l'utilisateur actuellement connecté.

Pour CA Cohesion ACM, "Secret partagé" est le secret utilisé pour accéder à CA cohesion ACM, s'il est requis. Cette valeur remplace {mot_de_passe} dans l'URL.

Remarque : Pour plus d'informations sur la définition du RDG, reportez-vous au *Manuel de mise en oeuvre de CA Cohesion ACM*.

Shared Secret

Spécifie les informations partagées entre CA CMDB et le RDG. Cette valeur remplace {mot_de_passe} dans l'URL. Pour les RDG de CA Cohesion ACM, la valeur doit correspondre à la valeur du "com.cendura.security.oneclickauth.secret". Pour plus d'informations sur la création d'un secret partagé, reportez-vous à la section "Intégration à CA CMDB" du *Manuel de mise en oeuvre de CA Cohesion ACM*. Requis pour la visionneuse CMDBf.

Espace de nom CMDBf

Spécifie l'ID ID federated_asset_id qui est transféré à la requête comme ID local. Pour CA CMDB, la valeur est http://cmdb.ca.com/r1.

CMDBf Timeout

(Facultatif) Spécifie la limite temporelle pour la demande de terminal CMDBf. La valeur par défaut est dix (10) secondes.

URL à lancer

Valeur par défaut de http://{nom_hôte}:{port}/{chemin}?{paramètres}. Pour quelques RDG, cette valeur peut au besoin être remplacée pour prendre en compte des conditions de configuration spécifiques. Obligatoire pour le lancement en fonction du contexte.

Pour le mdr_name APM et la mdr_class GLOBAL, la valeur est http://{nom_hôte}:{port}/{chemin}?{paramètres}.

Pour le mdr_name ITAM et la mdr_class GLOBAL, la valeur est http://{nom_hôte}:{port}/{chemin}?{paramètres}.

Pour la mdr_class Cohesion, la valeur par défaut est : http://*nom_hôte_cmdb*:*port_cmdb*/{chemin}?{paramètres}

où :

nom_hôte_cmdb est le nom d'hôte, le nom DNS ou l'adresse IP du serveur Web CA CMDB. Par défaut, cette valeur est définie sur le nom d'hôte actuel en train d'accéder au serveur Web CA CMDB.

port_cmdb est le port TCP/IP du serveur Web CMDB. Par défaut, cette valeur est définie sur le numéro de port ayant actuellement accès au serveur Web CA CMDB.

Remarque : Si vous avez activé la prise en charge SSL pour CA Cohesion ACM, définissez l'URL sur :

"http://nom_hôte:port/{chemin}?{paramètres}+https=yes"

Pour obtenir des informations sur l'activation de la prise en charge HTTPS de CA Cohesion ACM, reportez-vous à la rubrique d'aide en ligne de CA Cohesion ACM Création du certificat HTTPS et Activation de HTTPS.

Point terminal CMDBf

Indique le terminal de service de requête pour RDG. Requis pour la visionneuse CMDBf et la récupération de données RDG mises à jour. Si vous utilisez CA CMDB comme fournisseur de RDG, la valeur est http://cmdb_hostname:cmdb_port/axis/services/QueryPort.

4. Cliquez sur Enregistrer.

   Le RDG est défini.

Définitions de l'URL RDG

La valeur par défaut de l'URL à lancer est "http://{nom_hôte}:{port}/{chemin}?{paramètres}". Elle peut être modifiée comme nécessaire pour prendre en compte des éléments propres à un RDG. L'URL est requise pour le "lancement dans le contexte".

Pour mdr_name APM ou ITAM et mdr_class GLOBAL, la valeur par défaut est :

```
http://{nom_hôte}:{port}/{chemin}?{paramètres}
```

Pour la mdr_class Cohesion, la valeur par défaut est

"http://*nom_hôte_cmdb*:*port_cmdb*/{chemin}?{paramètres}"

cmdb_hostname

Spécifie le nom d'hôte, le nom DNS ou l'adresse IP du serveur Web CA CMDB. Sa valeur par défaut est le nom de l'hôte qui accède actuellement au serveur Web CA CMDB.

cmdb_port

Spécifie le port TCP/IP du serveur Web CA CMDB. Sa valeur par défaut est le numéro de port actuel utilisé pour accéder au serveur Web CA CMDB.

Si vous avez activé la prise en charge SSL pour CA Cohesion ACM, définissez l'URL sur :

```
"http://nom_hôte:port/{chemin}?{paramètres}+https=yes"
```

Remarque : Pour plus d'informations sur l'activation de la prise en charge HTTPS pour CA Cohesion ACM, reportez-vous à l'Aide en ligne de CA Cohesion ACM.

URL de lancement du RDG

Par défaut, l'URL de lancement du RDG a la valeur suivante :

```
http://{nom_hôte}:{port}/{chemin}?{paramètres}
```

Vous pouvez modifier cette expression en fonction des éléments propres à un RDG. L'URL est requise pour le lancement en contexte.

- Pour mdr_name APM ou ITAM et mdr_class GLOBAL, la valeur par défaut est :

  ```
  http://{nom_hôte}:{port}/{chemin}?{paramètres}
  ```

- Pour la mdr_class Cohesion, la valeur par défaut est

  "http://*nom_hôte_cmdb*:*port_cmdb*/{chemin}?{paramètres}"

  cmdb_hostname

  Nom d'hôte, nom DNS ou adresse IP du serveur Web CA CMDB. Sa valeur par défaut est le nom de l'hôte qui accède actuellement au serveur Web CA CMDB.

  cmdb_port

  Port TCP/IP du serveur Web CA CMDB. Sa valeur par défaut est le numéro de port actuel utilisé pour accéder au serveur Web CA CMDB.

  Si vous avez activé la prise en charge SSL pour CA Cohesion ACM, définissez l'URL sur :

  ```
  "http://nom_hôte:port/{chemin}?{paramètres}+https=yes"
  ```

  Remarque : Pour plus d'informations sur l'activation de la prise en charge HTTPS pour CA Cohesion ACM, reportez-vous à l'Aide en ligne de CA Cohesion.

Définition des paramètres de lancement pour la substitution de l'URL

Lors de la définition d'un RDG, les paramètres suivants peuvent être utilisés pour créer son URL à afficher. Ces paramètres sont remplacés par leurs valeurs appropriées lors de leur exécution. Ces variables doivent être spécifiées dans les champs décrits précédemment.

nom_hôte est le nom d'hôte du RDG issu de la définition du RDG.

alarm_id est l'adresse IP du CI sélectionné.

federated_asset_ID est l'identificateur unique du CI sélectionné dans le RDG.

cmdb_asset_id est l'ID d'actif pour le CI.

port est le numéro de port du RDG issu de la définition du RDG.

userid est l'ID d'utilisateur issu de la définition du RDG. Si cette valeur est laissée vide, l'ID de l'utilisateur prend par défaut la valeur de l'ID de l'utilisateur actuellement connecté.

password est le secret partagé issu de la définition du RDG.

mdr_name est le nom de RDG issu de la définition du RDG.

mdr_class est la classe de RDG issue de la définition du RDG.

class est la classe du CI sélectionné.

family est la famille du CI sélectionné.

path est le chemin décrit dans la définition du RDG.

name est le nom du CI sélectionné.

model est le modèle du CI sélectionné.

manufacturer est le fabricant du CI sélectionné.

itam_ticketid est l'ID de ticket pour se connecter à CA APM.

Exemple : Lancement d'un RDG

Un utilisateur CA CMDB consulte un CI serveur appelé serveur1, qui est mappé à une application développée en interne appelée Comet. Comet identifie serveur1 de façon unique par serveur:serveur1.

Comet est définie comme un RDG avec les propriétés ci-dessous.

- Nom d'hôte : ServeurComet
- Port : 80
- Chemin : index.php
- Paramètres : item={id_actif_fédéré}
- url_lancement : http://{nom_hôte}:{port}/{chemin}?{paramètres}

Dans CA CMDB, lorsque l'utilisateur clique sur le bouton Comet dans l'onglet Attributs du CI serveur1, une fenêtre de navigateur Web ouvre l'URL suivante.

http://ServeurComet:80/index.php?item=serveur:serveur1

Paramètres pour la substitution de l'URL

Lors de la définition d'un RDG, les paramètres suivants peuvent être utilisés pour créer son URL à afficher. Ces paramètres sont remplacés par leurs valeurs appropriées lors de leur exécution. Ces variables doivent être spécifiées dans les définitions de champ du RDG.

{nom_hôte}

Spécifie le nom d'hôte du RDG issu de la définition du RDG.

{alarm_id}

Spécifie l'adresse IP du CI sélectionné.

{federated_asset_ID}

Spécifie l'identificateur unique du CI sélectionné dans le RDG.

{cmdb_asset_id}

Spécifie l'ID d'actif pour le CI.

{port}

Spécifie le nom d'hôte du RDG issu de la définition du RDG.

{userid}

Spécifie l'ID d'utilisateur issu de la définition du RDG. Si cette valeur est laissée vide, l'ID de l'utilisateur prend par défaut la valeur de l'ID de l'utilisateur actuellement connecté.

{password}

Spécifie le secret partagé issu de la définition du RDG.

{mdr_name}

Spécifie le nom du RDG de la définition de RDG.

{mdr_class}

Spécifie la classe du RDG de la définition de RDG.

{class}

Spécifie la classe du CI sélectionné.

{family}

Spécifie la famille du CI sélectionné.

{path}

Spécifie le chemin d'accès comme décrit dans la définition du RDG.

{name}

Spécifie le nom du CI sélectionné.

{model}

Spécifie le modèle du CI sélectionné.

{manufacturer}

Spécifie le fabricant du CI sélectionné.

Exemple : utilisez des paramètres pour la substitution de l'URL

Un utilisateur CA CMDB consulte un CI serveur appelé serveur1, qui est mappé à une application développée en interne appelée Comet. Comet identifie serveur1 de façon unique par serveur:serveur1.

Comet est définie comme un RDG avec les propriétés ci-dessous.

- Nom d'hôte : ServeurComet
- Port : 80
- Chemin : index.php
- Paramètres : item={id_actif_fédéré}
- url_lancement : http://{nom_hôte}:{port}/{chemin}?{paramètres}

Dans CA CMDB, lorsque l'utilisateur clique sur le bouton Comet dans l'onglet Attributs du CI serveur1, une fenêtre de navigateur Web ouvre l'URL suivante.

```
http://ServeurComet:80/index.php?item=serveur:serveur1
```

Federation et le chargeur général de ressources

Lorsque le chargeur général de ressources est utilisé, les balises XML suivantes doivent être renseignées pour chaque CI du document XML. Ces balises s'appliquent à chaque famille RDG.

- <mdr_name>
- <mdr_class>
- <federated_asset_id>

Remarque : CA Cohesion ACM fournit automatiquement les variables mdr_name, mdr_class et federated_asset_id.

Si ces informations ne sont pas présentes dans le fichier XML, le "lancement dans le contexte" n'est pas possible car l'origine du CI ne peut pas être déterminée.

Pour identifier la source d'un CI, vous pouvez modifier le fichier XML avant qu'il ne soit utilisé en entrée par le chargeur général de ressources. Vous pouvez utiliser un éditeur de texte pour modifier le XML et faire une modification globale. Cette tâche peut également être réalisée par programmation.

Remarque : Pour plus d'informations sur l'identification RDG et le chargeur général de ressources, reportez-vous au *Manuel de référence technique de CA CMDB*.

Fédération d'un CI

Si des CI sont chargés dans CA CMDB avant que leur RDG correspondant ne soit défini, ils sont non fédérés, c'est-à-dire qu'ils ne sont pas encore connectés à un RDG et qu'ils ne prennent pas encore en charge le "lancement dans le contexte".

Pour fédérer un CI

1. Définissez le RDG requis.
2. Effectuez l'une des opérations ci-dessous.
   - Mappez manuellement le CI.
   - Relancez le rapport CA Cohesion ACM qui a créé le CI, en spécifiant Autoriser la mise à jour de CI existants pour le rapport.

     Remarque : Pour plus d'informations sur les rapports de CA Cohesion ACM, reportez-vous au *Manuel de présentation de CA Cohesion ACM*.
3. Relancez le chargeur général de ressources, en spécifiant le même fichier d'entrée que celui utilisé pour créer les CI.

   Le moteur de rapprochement CA CMDB fusionne les informations RDG dans les CI existants.
4. Créez un document XML qui décrit le CI et son RDG, puis exécutez le chargeur général de ressources en mode de mise à jour.

   Le moteur de rapprochement CA CMDB fusionne alors les nouvelles informations dans le CI existant. Le CI existant est fédéré.

Exemple : spécifiez l'emplacement du CI

Vous devez vérifier que le moteur de rapprochement dispose de suffisamment d'informations pour trouver le CI à mettre à jour. Dans l'exemple suivant, les balises de fin sont supprimées et des espaces sont ajoutés pour une meilleure lisibilité.

```
<ci>
   <name>         serveur3
   <mac_address>
   <serial_number>
   <asset_num>
   <dns_name>
   <mdr_name>     mdr_un
      <mdr_class> Cohesion
</ci>
```

Définition de plusieurs RDG pour un CI au moyen du chargeur général de ressources

Vous pouvez définir plusieurs RDG pour un CI en utilisant le chargeur général de ressources.

Pour définir plusieurs RDG associés à un CI unique, répétez dans le document XML le noeud <ci>, en spécifiant dans chaque noeud dupliqué un nom de RDG et une classe RDG différents. En d'autres termes, chaque RDG doit fournir ses attributs, indépendamment de tous les autres RDG qui fournissent des données au CI.

Exemple : définissez plusieurs RDG pour un CI

Si RDG1 et RDG2 fournissent tous deux des données au CI serveur2, le document XML doit présenter un aspect similaire à l'exemple ci-dessous. Dans cet exemple, les balises de fin sont supprimées et des espaces sont ajoutés pour une meilleure lisibilité.

```
<ci>
   <name>      serveur2
   <mdr_name>  rdg1
   <mdr_class> Cohesion
   <diskspace> 500 Go
   <disktype>  SCSI-3
</ci>
<ci>
   <name>     serveur2
   <mdr_name> rdg2
   <mdr_class>Service Assure
   <sla>
</ci>
```

CA CMDB rapproche les deux CI ci-dessus dans le même CI et associe chacun des deux RDG à ce CI unique.

Remarque : Les CI peuvent être importés en une ou deux exécutions du chargeur général de ressources.

Mappage des CI RDG et des CI CA CMDB

Une fois un CI défini manuellement au moyen de l'option Fichier, Nouvel élément de configuration, vous devez définir manuellement le mappage entre ce CI et le CI du RDG fédéré. Deux méthodes sont possibles pour associer un CI à un RDG.

- Modifiez le CI.
- Utilisez le noeud Mappage d'éléments de configuration fédérés dans l'onglet Administration de CA CMDB.

Pour créer un mappage en modifiant le CI

1. Affichez la page Détails du CI pour le CI que vous souhaitez associer au RDG.
2. Cliquez sur Modifier.
3. Affichez l'onglet Attributs.
4. Cliquez sur Ajouter un RDG.

   Le CI est associé au RDG.

Pour créer un mappage en utilisant la page Mappage de CI fédérés

1. Cliquez sur l'onglet Administration de CA CMDB.
2. Ouvrez le noeud Référentiel de données de gestion.
3. Sélectionnez le noeud Mappage de CI fédérés.

   La Liste des mappages de CI fédérés apparaît.
4. Cliquez sur Créer.

   La page "Créer un mappage de CI fédérés pour" apparaît.
5. Associez le CI au RDG en remplissant les champs Mappage de CI fédérés :

   Nom CI

   Spécifie le nom à utiliser pour identifier le CI.

   ID de l'actif fédéré

   Spécifie l'identificateur de type chaîne utilisé par le RDG source pour identifier ce CI. L'identificateur est déterminé par le logiciel RDG.

   Nom du RDG

   Spécifie le nom qui identifie le RDG (et son bouton RDG).

   Actif

   Indique si ce mappage est activé ou non. Les mappages ne peuvent pas être supprimés, mais uniquement désactivés.
6. Cliquez sur Enregistrer.

   Le mappage entre ce CI et le CI dans le RDG fédéré est défini.

Configuration des RDG pour la visionneuse CMDBf

Avant de pouvoir utiliser la visionneuse CMDBf, vous devez configurer vos fournisseurs RDG fédérés de la façon suivante pour qu'ils pointent vers le service de requête CMDBf :

- Les RDG externes doivent fournir un service de requête capable de traiter la requête InstanceIdConstraint.
- Le nom de Bouton, le nom du RDG et la classe du RDG sont requis pour afficher le bouton de la visionneuse CMDBf sur la page Détail de l'élément de configuration.
- La classe de RDG doit être définie sur **cmdbf**.
- Pour CA CMDB, l'espace de noms CMDBf doit être défini sur **http://cmdb.ca.com/r1**. Pour d'autres CMDB et des RDG, reportez-vous à la documentation appropriée.
- La temporisation est facultative. La valeur par défaut est dix (10) secondes.
- Pour afficher un bouton Récupérer actif sur la vue fédérée, vous devez définir les valeurs CMDBf de terminal, d'ID d'utilisateur et de secret partagé.

Remarque : Un système CA CMDB existant peut être configuré comme un fournisseur de CMDBf en spécifiant un terminal CMDBf pour http://nom_serveur:port/axis/services/QueryPort, où

- nom d'hôte désigne l'ordinateur sur lequel CA CMDB est installé (nom de l'hôte local ou de l'ordinateur), et où
- port désigne le port sur lequel CA CMDB est configuré.

Lancement de l'interface de navigateur Web RDG

Une fois le mappage créé entre un CI et un RDG, un bouton est automatiquement placé dans l'onglet Attributs. Si plusieurs RDG sont associés au CI, plusieurs boutons apparaissent.

Lorsque l'utilisateur clique sur un bouton RDG, une nouvelle page s'ouvre et l'URL RDG apparaît. Toutes les parties de cette URL sont remplacées par les valeurs de la définition RDG.

Exemple : lancement de CA Cohesion

Lorsqu'un CI a été associé correctement à son RDG, un bouton Cohesion s'affiche sur l'onglet Attributs. Si un bouton n'apparaît pas dans l'onglet Attributs, vérifiez le mappage du CI affiché. Vérifiez qu'un mappage existe pour ce CI et que le RDG cible dispose d'une URL qui peut être lancée. Si l'utilisateur clique sur le bouton pour lancer le RDG, une nouvelle fenêtre s'ouvre pour l'URL cible afin de lancer CA Cohesion.

Intégration CA Cohesion

Considérez les éléments suivants en intégrant CA Cohesion ACM avec CA CMDB :

- Intégration de Cohesion à CA CMDB

  Remarque : Pour plus d'informations sur l'intégration Cohesion-CA CMDB, reportez-vous au *Manuel de mise en oeuvre de CA Cohesion ACM*.

- Importation de CI depuis un RDG Cohesion

  Remarque : Pour plus d'informations sur l'importation de CI à partir d'un RDG Cohesion, reportez-vous à l'Aide en ligne disponible depuis l'onglet Modèles de rapports dans les rapports CA Cohesion ACM.

- Lancement dans le contexte de RDG Cohesion

  Pour un fonctionnement optimal de l'intégration du lancement dans le contexte avec CA Cohesion ACM, il est recommandé d'utiliser l'onglet Administration de CA CMDB pour définir le RDG Cohesion *avant* d'exécuter le rapport Cohesion CMDB.

  Remarque : Comme CA Cohesion ACM ne prend pas en charge un ID d'actif fédéré unique pour les CI Carte réseau ou Système de fichiers, Cohesion ne prend pas en charge le lanceur RDG pour ces CI. Un CI Carte réseau ou Système de fichiers Cohesion n'affiche donc pas de bouton de lancement de chargeur général de ressources, même s'il a été importé avec succès.

Chapitre 12: Gestion des services Web

Important : Pour de plus amples renseignements sur les services Web, reportez-vous au Manuel de référence technique de CA SDM.

Ce chapitre traite des sujets suivants :

Gestion des services Web (page 565)
Composants CA SDM (page 566)
Conseils pour les clients des services Web SOAP (page 566)
Configuration des services Web SOAP (page 569)
Sécurité des services Web (page 571)
Traitement des erreurs SOAP (page 573)
Installation des services Web (page 577)
Caractéristiques externes (page 577)
Objets (page 597)
méthodologie ITIL (page 602)
Utilisation des services Web (page 605)

Gestion des services Web

Les *services Web* sont constitués d'un ensemble de normes d'échange de données qui permettent la communication entre les produits, même si ceux-ci se trouvent dans des environnements d'exploitation différents. Cette capacité est donc comparable à la navigation Web sur un ordinateur personnel : tous les sites distants sont accessibles, qu'ils soient hébergés sur Solaris, AIX, Windows, etc. De la même manière, les services Web permettent aux produits d'être reliés à divers serveurs par l'entremise du protocole HTTP, et ce quel que soit l'environnement d'exploitation. Ainsi, un produit Microsoft Office peut communiquer avec un programme hébergé sur un serveur UNIX et une page Java Server peut accéder à un serveur sous Windows. Ce type de communication, possible à partir de n'importe quelle plate-forme, offre de grandes possibilités d'intégration.

Les services Web bénéficient de cette technologie : la plupart des produits peuvent accéder à CA SDM et aux Gestion des connaissances. Les clients de services Web peuvent créer des tickets, mettre à jour des composants, effectuer des recherches dans la base de connaissances, etc.

Composants CA SDM

CA SDM fournit les fichiers d'installation pour cette version des services Web de J2EE dans le répertoire suivant :

<NX_ROOT>/sdk/websvc/R11

Remarque : <NX_ROOT> spécifie la racine du chemin d'installation de CA SDM.

Conseils pour les clients des services Web SOAP

Le répertoire Samples de l'installation CA SDM fournit un exemple d'application cliente Java pour des services Web. Cet exemple assiste les développeurs dans le développement d'applications clientes de services Web.

De nombreuses méthodes de services Web requièrent des tableaux comme paramètres d'entrée. Par exemple, la méthode createIssue() permet un tableau vide pour propertyValues. Ces tableaux sont parfois facultatifs, mais le service requiert un tableau vide pour un transfert correct. Lorsque vous utilisez Visual Studio .NET pour accéder aux services Web, indiquez un tableau vide à l'aide de l'un des tableaux suivants :

Langage C#

```
String[] emptyArray = new string[0];
```

Visual Basic .NET

```
Dim emptyArray As String() = {}
```

Java

```
ArrayOfString attr = new ArrayOfString();
attr.setString(new String[0]);
ArrayOfString est une classe propriétaire.
```

emptyArray peut ensuite être transféré vers les paramètres de tableau qui acceptent les tableaux vides.

Remarque : Les services Web de CA SDM utilisent la mise en oeuvre Apache des normes établies par le World Wide Web Consortium (W3C). Idéalement, un client doit être en mesure d'accéder aux services quel que soit le type d'environnement d'exploitation utilisé. Toutefois, la mise en oeuvre est susceptible de varier selon le fournisseur. De nombreux environnements de programmation proposent un outil permettant de générer des classes de mandataire à partir d'une description Web Services Description Language (WSDL).

Informations complémentaires :

Clients Java (page 567)

Clients Java

TableOfContents.doc dans $NX_ROOT/samples/sdk/websvc répertorie plusieurs exemples de programmes Java.

Chaque exemple de programme contient des remarques expliquant comment le compiler et l'exécuter à l'aide des fichiers de script run_java_test_bat.txt (Windows) et run_java_test_sh.txt (UNIX). Ces scripts montrent comment utiliser org.apache.axis.wsdl.WSDL2Java pour générer les fichiers stub côté client des services Web de CA SDM.

Le paramètre –w est obligatoire pour générer correctement les fichiers stub lors de l'utilisation d'Axis 1.4. L'exécution de WSDL2Java, ainsi qu'elle est expliquée, génèrera les fichiers stub dans le sous-répertoire com/ca/www/UnicenterServicePlus/ServiceDesk. Les fichiers suivants sont créés :

- ArrayOfInt.java
- ArrayOfString.java
- ListResult.java
- USD_WebService.java
- USD_WebServiceLocator.java
- USD_WebServiceSoap.java
- USD_WebServiceSoapSoapBindingStub.java.

Importez ces classes avec l'instruction suivante :

```
import com.ca.www.UnicenterServicePlus.ServiceDesk.*;
```

De nombreuses méthodes de services Web utilisent des paramètres de type ArrayOfString, une classe propriétaire. Par exemple, les paramètres attrVals, propertyValues et paramètres d'attributs de la méthode createRequest() sont tous des paramètres ArrayOfString.

Pour définir les valeurs dans une variable ArrayOfString, instanciez la variable, puis utilisez setString() comme suit :

```
ArrayOfString attrVals = new ArrayOfString();
attrVals.setString(new String[]{"customer", customerHandle, "description",
"description text"});
```

Pour le définir sur une valeur vide

```
attrVals.setString(new String[0]);
```

Utilisez une variable de type ListResult, une autre classe propriétaire, en tant que valeur renvoyée par les méthodes de liste : doQuery(), getRelatedList(), getNotificationsForContact(), getPendingChangeTaskListForContact() et getPendingIssueTaskListForContact(). Un ListResult contient des éléments listHandle et listLength, qui peuvent être récupérés à l'aide de getListHandle() et getListLength(), comme indiqué dans cet exemple :

```
ListResult doQueryResult = new ListResult();
doQueryResult = USPSD.doQuery(sid, "iss", "active = 1");
int listHandle = doQueryResult.getListHandle() ;
int listLength = doQueryResult.getListLength() ;
```

La méthode getListValues() utilise listHandle et récupère les valeurs provenant d'un sous-ensemble de la liste.

Le paramètre Handles de la méthode de freeListHandles() est un ArrayOfInt, une autre classe propriétaire. Appelez freeListHandles() à l'aide du listHandle obtenu depuis ListResult :

```
ArrayOfInt handleList = new ArrayOfInt();
handleList.setInteger(new java.lang.Integer []{ new java.lang.Integer(listHandle)
});
USPSD.freeListHandles(sid, handleList);
```

Certaines méthodes utilisent des paramètres passés par référence de type javax.xml.rpc.holders.StringHolder. Par exemple, createRequest() a deux paramètres de ce type, à savoir NewRequestHandle et NewRequestNumber.

```
StringHolder NewRequestNumber = new StringHolder();
StringHolder NewRequestHandle = new StringHolder();
String result;
result = USPSD.createRequest(sid, creatorHandle, attrVals, propertyValues, template,
attributes, NewRequestHandle, NewRequestNumber);
```

Vous pouvez vous procurer le descripteur et le numéro de référence (ref_num) de la requête auprès, respectivement, de NewRequestHandle.value et de NewRequestNumber.

Configuration des services Web SOAP

Vous pouvez configurer les services Web SOAP de CA SDM avec des entrées dans les fichiers de configuration Web spéciaux. La table suivante récapitule les noms et les descriptions des options de configuration :

Nom de l'option	Description
design_mode_stubs	Définit le service Web sur le *mode Conception* (CA SDM uniquement).
require_secure_logon	Les méthodes Web login() et loginService() doivent être appelées selon un protocole sécurisé, comme https.
require_secure_connection	Chaque méthode Web doit être appelée selon un protocole sécurisé.
disable_user_logon	Les méthodes Web login() et loginService() sont désactivées de sorte que seule la méthode loginServiceManaged() peut être utilisée pour se connecter.

CA SDM ajoute une protection à l'intégrité du serveur Tomcat en cours d'exécution en vérifiant la longueur des valeurs d'attribut transmises à des méthodes de service Web. Par défaut, les appels de service Web renvoient une erreur Axis si la longueur d'une valeur d'attribut est supérieure à 900 000 octets.

Définissez les paramètres suivants dans le fichier deploy.wsdd :

fatal_max_string_length

Définit la longueur de la valeur d'attribut maximale qui sera acceptée par une méthode de service Web.

Valeur par défaut : 900 000 octets

validate_parameters

Détermine s'il convient d'effectuer une vérification de la longueur de la valeur d'attribut. Définissez le paramètre sur 0 pour désactiver la validation.

Valeur par défaut : 1 (activé)

exception_methods

Affiche une liste délimitée par des virgules de méthodes de service Web dépourvues de validation de la longueur de la valeur d'attribut.

Renseignements supplémentaires :

Redéploiement des services Web (page 570)

Redéploiement des services Web

Les nouveaux paramètres de configuration prennent effet lorsque les services Web de CA SDM sont redéployés. Effectuez les opérations suivantes pour redéployer les services Web :

1. Ouvrez une invite de commande, puis définissez la variable d'environnement CLASSPATH pour inclure les fichiers .jar Axis requis fournis dans <NX_ROOT>/java/lib.

   Par exemple, pour la définir sous Windows, exécutez la commande suivante :

   ```
   set AXISHOME=%NX_ROOT%\java\lib
   set classpath=
   %AXISHOME%\axis.jar;%AXISHOME%\jaxrpc.jar;%AXISHOME%\saaj.jar;%AXISHOME%\comm
   ons-logging.jar;%AXISHOME%\commons-discovery.jar;%AXISHOME%\wsdl4j.jar;%AXISH
   OME%\log4j-1.2.8.jar;%classpath%;
   ```

2. Remplacez le répertoire par <NX_ROOT>/sdk/websvc/R11 et exécutez les commandes suivantes :

   ```
   java org.apache.axis.client.AdminClient undeploy.wsdd
   java org.apache.axis.client.AdminClient deploy.wsdd
   ```

3. Recyclez Tomcat en redémarrant le service CA SDM. Vous pouvez éviter l'arrêter de l'ensemble du système CA SDM en redémarrant Tomcat simplement à l'aide des commandes suivantes :

   ```
   pdm_tomcat_nxd –c stop
   pdm_tomcat_nxd –c start
   ```

   Le service Web est redéployé.

4. Vérifiez que le service est déployé, en affichant la page répertoriant les services Axis qui se trouve par défaut à l'adresse URL suivante :

   ```
   http://<nom_serveur>:<port>/axis/services
   ```

   Remarque : L'URL exacte dépend de vos paramètres d'installation.

Sécurité des services Web

Lors du déploiement des services Web, consultez les remarques de sécurité importantes. En cas d'utilisation du protocole HTTP, la configuration par défaut n'est pas sécurisée, comme c'est le cas pour toutes les informations sur les appels de services Web échangées par le client et le serveur sur le réseau, en texte brut, à l'aide du protocole HTTP. Cela inclut non seulement des données d'application, telles que des descriptions de ticket et des noms de contact, mais également les identificateurs de session de service Web (SID). Selon les méthodes de connexion à l'application de service Web utilisées, des mots de passe peuvent être inclus.

Nous conseillons vivement aux administrateurs qui déploient des services Web de lire attentivement ces informations et de réaliser des actions de configuration supplémentaires au niveau de l'application et du réseau afin de sécuriser leur environnement de service Web.

Important : la configuration par défaut du service Web utilisée avec HTTP n'est pas sécurisée et elle est donc vulnérable aux menaces de sécurité telles que le vol des mots de passe, le blocage de session et l'espionnage des données.

Le déploiement des services Web doit prendre en considération trois questions de sécurité interdépendantes :

- Quelles sont les méthodes d'authentification d'accès (niveau applicatif) que ce déploiement doit prendre en charge ?
- Quelles sont les fonctions de sécurité supplémentaires dont ce déploiement a besoin en matière de mise en réseau ?
- Comment ces exigences seront-elles appliquées par l'intermédiaire des options de configuration du service Web ?

Voici une description de chacune des fonctions de sécurité :

- **Méthodes d'authentification au niveau de l'application de service Web :** pour pouvoir accéder aux services Web, une application cliente de service Web doit être authentifiée auprès de l'application de service Web. Les services Web proposent deux méthodes d'authentification d'accès. Il est possible de recourir à la combinaison nom d'utilisateur/mot de passe ou à la technologie d'infrastructure de clés publiques (PKI). Ces deux méthodes fonctionnent en collaboration avec le composant de gestion et contrôle d'accès des services Web, en utilisant notamment les politiques d'accès. L'authentification et la gestion d'accès sont les fonctions de sécurité les plus importantes des services Web.

La commande de configuration de la sécurité suivante permet de désactiver les méthodes d'authentification recourant à la combinaison nom d'utilisateur/mot de passe :

```
disable_user_logon
```

Avant d'activer cette option, l'administrateur doit déterminer si chaque client de service Web pour lequel une entreprise demande un accès aux services Web peut réellement prendre en charge l'autre méthode d'authentification, c'est-à-dire la méthode de connexion basée sur PKI. L'avantage principal de la technologie d'infrastructure de clés publiques (PKI) réside dans le fait que les applications clientes de services Web ne nécessitent pas que le système *assure la gestion* des comptes d'utilisateur (maintenance, stockage et transmission de leurs mots de passe).

- **Configuration de la sécurité pour la mise en réseau :** qu'il s'agisse de la méthode d'authentification par nom d'utilisateur/mot de passe ou par infrastructure de clés publiques (PKI), vous remarquerez que l'identificateur de session renvoyé par la méthode de connexion choisie (ainsi que toutes les informations qui en découlent) est transmis en texte brut lorsque le protocole HTTP est utilisé. De plus, lorsque la méthode d'authentification par nom d'utilisateur/mot de passe est utilisée, l'application client du service Web envoie le mot de passe aux services Web sans le protéger (en texte brut). Le W3C n'a pas recommandé de norme pour la sécurité des services Web pendant la phase de développement du produit. C'est pourquoi ces mises en oeuvre de services Web n'utilisent pas WS-Security pour créer un contexte sécurisé. Il est donc recommandé d'utiliser le protocole SSL/TLS de point à point ainsi que d'autres mécanismes de sécurité au niveau du réseau (par exemple, le protocole IPSec) afin de protéger le texte transmis lors des échanges d'authentification au niveau de l'application qui, sans cela, apparaît en clair, ainsi que l'identification et les données de session transmises ultérieurement.

  Important : Il est conseillé d'utiliser le protocole SSL (ou https) lors du déploiement des services Web afin de protéger les échanges d'authentification au niveau de l'application ainsi que les transmissions ultérieures d'identification et de données de session.

- **Configuration du service Web :** les deux commandes de configuration de sécurité suivantes sont prises en charge afin de permettre aux administrateurs de sécuriser les communications à l'aide d'un protocole au niveau de l'application de services Web :

  ```
  require_secure_logon
  ```

  Cette fonction de sécurité nécessite que vous utilisiez un protocole SSL (ou https) pour appeler les méthodes Login() et LoginService(). Elle constitue également une méthode pratique de protection du nom d'utilisateur et du mot de passe, tout en évitant la surcharge du protocole SSL pour les autres services Web.

Important : si vous utilisez la commande require_secure_logon, l'application de services Web ne confirmera pas que la sécurisation des communications par protocole est appliquée pour les méthodes autres que Login() et LoginService(). Si vous ne prenez pas d'autres précautions, il se peut que les autres méthodes de services Web soient appelées de façon non sécurisée, ce qui accroît la vulnérabilité aux menaces sur la sécurité.

`require_secure_connection`

Cette fonction vous oblige à utiliser le protocole SSL pour accéder à n'importe quelle partie du service Web. Si le protocole https est requis, mais reste inutilisé, une erreur SOAP reprenant le code UDS_SECURE_CHANNEL_REQUIRED est renvoyée.

Remarque : Pour plus d'informations sur la configuration du protocole SSL, reportez-vous à la documentation du conteneur de servlets J2EE.

Informations complémentaires :

Caractéristiques externes (page 577)

Traitement des erreurs SOAP

Si une erreur affecte une méthode des services Web, une erreur SOAP est renvoyée. L'erreur SOAP est la méthode la plus courante d'envoi d'informations concernant les exceptions.

Le message d'erreur contient des éléments normalisés <Message> et <Code>, mais l'élément comportant le plus d'informations est l'élément <Detail>. L'élément <Detail> renferme les éléments <ErrorCode> et <ErrorMessage>. L'élément <ErrorCode> renvoie un code d'erreur énuméré spécifique au produit CA SDM ou aux Gestion des connaissances. L'élément <ErrorMessage> comporte une chaîne en français qui décrit les erreurs. Les éléments <ErrorMessage> s'adressent plus particulièrement aux développeurs, tandis que des messages plus clairs s'affichent pour les utilisateurs.

L'exemple suivant présente une erreur SOAP renvoyée lorsqu'un paramètre incorrect est fourni pour la méthode getObjectValues() de CA SDM.

```
<soap:Fault>
    <faultcode>soap:Client</faultcode>
    <faultstring>Erreur lors de l'extraction avec la liste
    d'attributs:persistent_id,first_name,last_nameParamErrorHere<faultstring>
    <detail>
<ErrorCode>1001</ErrorCode>
<ErrorMessage> Erreur lors de l'extraction avec la liste d'attributs :
persistent_id,first_name,last_nameParamErrorHere </ErrorMessage>
    </detail>
    </soap:Fault>
```

Si vous utilisez un client créé à l'aide d'un code géré Microsoft .NET, l'échec de l'appel de services Web engendre une exception SOAPException. Toutes les erreurs annulent l'opération appelée.

Il arrive parfois que des erreurs soient rédigées par le conteneur de servlets et, par conséquent, qu'elles apparaissent dans les journaux de conteneurs de servlets. Dans d'autres cas, il arrive aussi que des informations sur les erreurs soient rédigées dans les journaux CA SDM. Ces journaux sont situés dans les sous-répertoires suivants :

- Dans le sous-répertoire /bopcfg/www/CATALINA_BASE/logs de l'installation de CA SDM.
- Dans le sous-répertoire /log de l'installation de CA SDM et dans tous ceux portant le préfixe stdlog.

Remarque : Il est recommandé de contrôler en permanence ces journaux ; en effet, le serveur peut y consigner ses propres erreurs sans les signaler aux services Web CA SDM.

Erreurs de verrouillage

Les objets de CA SDM sont verrouillés pendant les mises à jour. Les méthodes de mise à jour des objets (telles que updateObject() ou transfer()) peuvent renvoyer le code d'erreur de verrouillage suivant :

```
UDS_LOCK_ERR
```

Ce code indique qu'un autre utilisateur est en train de mettre à jour l'enregistrement. Le descripteur de l'utilisateur qui effectue le verrouillage est souvent renvoyé dans l'élément ErrorMessage.

Temporisations

Si la charge du serveur CA SDM est très élevée, le traitement d'une méthode peut être long. Dans de rares cas, une méthode peut ne jamais rien renvoyer, car un traitement effectué séparément n'a pas pu répondre ou une autre erreur s'est produite. Pour éviter tout blocage excessif, chaque méthode de service Web arrive à expiration après un certain nombre de secondes. La temporisation de la méthode de services Web correspond à la temporisation du serveur CA SDM, *et non* à celle d'un serveur Web, d'un réseau, etc.

Remarque : Les services Web ralentissent pendant quelques secondes lors du premier accès suivant le redémarrage du serveur d'applications J2EE. Cela se produit uniquement lors du premier appel de la méthode des services Web pendant que l'application s'initialise, charge les DLL, les bibliothèques, etc. Le renvoi des appels suivants est beaucoup plus rapide.

Si une méthode arrive expiration, elle renvoie le code d'erreur suivant :

```
UDS_TIMEOUT_ERR
```

L'opération n'est pas annulée ! Le serveur peut avoir reçu la requête ; il la traitera correctement, mais lentement. Ce type de problème peut se produire lorsque la méthode *doSelect()* est utilisée pour récupérer plusieurs milliers d'enregistrements.

Remarque : Pour plus d'informations sur la méthode *doSelect*, reportez-vous au *Manuel de référence technique de CA SDM*.

Codes d'erreur

Le tableau ci-dessous répertorie les valeurs que peut prendre la valeur <ErrorCode> dans une erreur SOAP renvoyée à la suite d'un appel de service Web.

Nom de l'erreur	Valeur	description
UDS_OK	0	Réussi.
UDS_FAILURE	1	Echec général, vérifiez les journaux système.
UDS_BAD_PARAM	1000	Un paramètre incorrect a été transmis à une méthode. Cette erreur se produit si un paramètre requis est manquant, si le type transmis est incorrect ou si la valeur utilisée n'est pas valide.
UDS_INTERNAL_ERR	1001	Indique qu'une erreur interne s'est produite. Une description de cette erreur se trouve dans le tableau de retour et les journaux d'activité.

Nom de l’erreur	Valeur	description
UDS_LOCK_ERR	1002	Tentative de mise à jour d’un objet verrouillé par un autre utilisateur ou un processus. En règle générale, l’ID du contact responsable du verrouillage de l’objet est renvoyé avec les données.
UDS_UPDATE_ERR	1003	Une erreur s’est produite lors de la mise à jour d’un objet. Assurez-vous que tous les attributs requis ont été définis et vérifiez le journal système.
UDS_CREATION_ERR	1004	Une erreur s'est produite lors de la création d'un objet. Assurez-vous que tous les attributs requis ont été définis et vérifiez les journaux système.
UDS_NOT_FOUND	1005	Une méthode de recherche n’a pas trouvé de correspondances ou n’a pas trouvé l’objet spécifié. Cela peut se produire si un descripteur incorrect ou non valide est transmis à une méthode.
UDS_SESSION_TIMEOUT	1006	Le délai de la méthode actuelle a expiré, le serveur CA SDM est peut-être très chargé, ou la méthode elle-même est peut-être incorrecte.
UDS_SERVER_GONE	1007	La connexion au serveur CA SDM a été perdue : les méthodes UDS ne peuvent plus fonctionner et toutes les références de la liste ont été perdues.
UDS_FETCH_ERR	1008	Une erreur s’est produite lors de l’extraction des données de la liste.
UDS_BAD_SESSION	1010	Un ID de session non valide a été utilisé.
UDS_CNTXT_TIMEOUT	1011	Le délai de l’ID de session a expiré.
UDS_SECURE_ CHANNEL_REQUIRED	1012	Les services Web (ou une méthode de service Web) exigent un accès par canal sécurisé (par exemple : SSL) alors qu'un canal non sécurisé est utilisé.
UDS_SECURITY_ VIOLATION	1013	L'opération tentée constitue une violation de la sécurité de CA SDM et a été abandonnée.
UDS_OVER_POLICY_ LIMIT	3002	La requête tentée a été refusée, car elle dépasse la limite définie dans la politique.

Installation des services Web

Selon le type de configuration, CA SDM installe les services Web pour les serveurs suivants :

- Conventionnelle : serveurs principal et secondaire. Ajoutez un moteur Web au serveur secondaire de sorte que les clients des services Web puissent utiliser une URL sur celui-ci.
- Disponibilité avancée : serveur d'applications

Les services Web utilisent le gestionnaire d'objets par défaut installé sur le serveur CA SDM. Pour utiliser d'autres gestionnaires d'objets, installez et définissez l'option *webservice_domsrvr* dans le gestionnaire d'options.

Remarque : Pour de plus amples renseignements sur l'ajout et la configuration de gestionnaire d'objets, de directeurs Web et de moteurs Web, reportez-vous au *Manuel d'administration*. Pour de plus amples renseignements sur l'installation et le paramétrage de l'option *webservice_domsrvr*, reportez-vous à l'*Aide en ligne*.

Activation de la phase de conception

Les services Web de CA SDM comprennent une fonction de configuration de la méthode stub destinée aux développeurs dans la version Java. Lorsqu'ils sont activés, les services Web ignorent le serveur de CA SDM et renvoient des données simulées pour les appels de méthode afin que les appels de services Web puissent être effectués sans exécuter un serveur CA SDM.

1. Modifiez deploy.wsdd de façon à ce qu'il ne fasse plus de commentaires sur les sections pour design_mode_stubs.
2. Inversez le déploiement et redéployez le serveur.
3. Redémarrez le serveur d'application.

   La fonction de phase de conception est activée.

Remarque : La fonction de phase de conception s'applique uniquement aux méthodes de services Web CA SDM.

Caractéristiques externes

CA SDM vous permet spécifier l'authentification de l'accès utilisateur et les fonctionnalités disponibles par le contrôle et la gestion de l'accès.

Authentification d’accès utilisateur

Les services Web de CA SDM proposent deux méthodes d'authentification d'accès. Celles-ci sont associées à la nouvelle fonction de contrôle et de gestion des accès qui utilise une stratégie d'accès.

Nom d’utilisateur/Mot de passe

Vérifie le nom d’utilisateur/mot de passe, comme indiqué dans les versions précédentes du produit.

Technologie d’infrastructure de clés publiques (PKI)

Vérifie que la personne demandant l’accès dispose d’une clé privée spécifique.

Important : Si vous prévoyez d'utiliser une application qui a accès à cette version des services Web de CA SDM, nous vous recommandons fortement de définir au préalable une politique d'accès aux services Web (y compris la valeur de code) dans CA SDM. Une politique d'accès par défaut comportant un code de politique DEFAULT est disponible lorsque CA SDM est installé et configuré.

Informations complémentaires :

Définition d'une politique d'accès (page 587)

Authentification par Nom d’utilisateur/Mot de passe

Si vous souhaitez utiliser l'authentification d'accès de type Nom d'utilisateur/Mot de passe, l'application utilisateur doit appeler l'une des deux méthodes de services Web suivantes afin d'accéder aux services Web de CA SDM.

Remarque : L'utilisateur connecté que vous spécifiez dans le paramètre de nomd'utilisateur (et non le contact mandataire indiqué dans la politique) est responsable des activités lancées au cours d'une session. La sécurité pour les groupes de fonctions et la partition des données sont appliquées à l’utilisateur connecté.

login (Username, Password)

Cette méthode, qui procède à une authentification d’accès par l'entremise du nom d’utilisateur et du mot de passe fournis, permet d’assurer la compatibilité ascendante. Un ID de session (SID) est renvoyé uniquement si l’accès est authentifié. Tous les appels de services Web suivants doivent inclure cet ID de session. La politique d'accès par défaut est ensuite appliquée à tous les accès aux services Web suivants qui portent le nom de l'ID de session.

Les champs Nom d’utilisateur et Mot de passe sont obligatoires. Les valeurs entrées dans ces champs doivent être au format texte brut.

loginService (Username, Password, Policy)

Cette méthode est similaire à la fonction de connexion (login) décrite précédemment : l'authentification d'accès est réalisée au moyen du nom d'utilisateur et du mot de passe fournis. Un ID de session est renvoyé uniquement si l'accès est authentifié. Cependant, une politique d'accès spécifique, identifiée dans le troisième paramètre, est appliquée afin de contrôler et de gérer tous les accès aux services Web suivants. Si le paramètre de la règle est vide, la règle par défaut est appliquée automatiquement.

Les champs Nom d'utilisateur et Mot de passe sont obligatoires. Les valeurs entrées dans ces champs doivent être au format texte brut. La règle est requise, mais elle peut être vide. Vous devez alors utiliser le format texte brut. Utilisez le code de règle défini dans une règle.

Le mode de validation d'une connexion dépend du *type d'accès* affecté au contact. L'objet Type d'accès est hébergé par CA SDM et définit le type de validation. Vous pouvez utiliser le produit pour afficher l'enregistrement du type d'accès. Vous pouvez également utiliser la méthode Web getAccessTypeForContact() pour récupérer des informations sur l'objet du type d'accès.

Remarque : Pour plus d'informations sur les types d'accès, reportez-vous au *Manuel d'administration*.

Authentification par l'entremise d'une infrastructure de clés publiques (PKI)

Si vous souhaitez utiliser l'authentification PKI, retenez que le contenu de la demande de connexion est crypté à l'aide d'une clé privée et ne peut être décrypté qu'avec la clé publique correspondante. La réponse à la demande de connexion est renvoyée sous forme de texte brut.

En règle générale, une règle est affectée à chaque application accédant aux services Web de CA SDM. Les services Web de CA SDM stockent des informations détaillées concernant une règle avec la clé publique d'un certificat numérique. Une application, telle que le souscripteur, utilise la clé privée du certificat numérique et le code de la règle (comme identifiant de la règle) pour assembler une demande de connexion.

loginServiceManaged (Policy, Encrypted_Policy)

Les services Web de CA SDM procèdent à l'authentification de l'utilisateur de la manière suivante : ils localisent la politique dans le code de politique en texte brut, extraient la clé publique du souscripteur associée au code de la politique, déchiffrent le code de la politique, font correspondre le contenu déchiffré avec le code de la politique et, enfin, ouvrent une session avec un serveur principal. L'ID de session (SID) en texte brut est renvoyé et peut être utilisé pour les appels de méthode suivants. Seul le souscripteur possède la clé privée correspondant à la clé publique associée stockée dans CA SDM.

Tous les appels de services Web suivants doivent inclure l'ID de session (SID) renvoyé. Le contact mandataire spécifié dans cette politique est responsable de toutes les activités des services Web lancées au cours de cette session. La sécurité pour les groupes de fonctions et la partition des données sont appliquées au contact mandataire.

Important : le paramètre Encrypted_Policy doit être au format texte BASE64. L'application utilisateur doit effectuer une conversion correcte à partir du format binaire.

Le champ Règle est obligatoire. Lorsque vous définissez ce champ, utilisez le code de règle en texte brut défini dans une règle. Le champ Encrypted_Policy (signature numérique du code de règle crypté à l'aide de la clé privée du souscripteur) est obligatoire. Lorsque vous définissez le champ Encrypted_Policy, utilisez l'algorithme SHA1 avec RSA pour obtenir la signature numérique.

Mise en oeuvre de loginServiceManaged dans Java

Le contenu suivant montre comment générer des certificats, puis utiliser ces certificats produits pour accéder aux services Web de CA SDM.

Dans l'exemple suivant, le processus de connexion s'effectue à l'aide du certificat CA SDM, puis procède à deux appels de services Web communs. L'appel de la méthode Services Web getBopsid() vous permet d'obtenir un jeton lié à un utilisateur spécifique. Ce jeton peut servir à se connecter à l'interface Web de CA SDM en tant qu'utilisateur associé sans être invité à entrer un mot de passe. Cela permet de mettre en place une intégration transparente entre les différentes applications.

Important : Le jeton BOPSID généré doit être utilisé rapidement car il expire au bout de 30 secondes.

Important : L'utilisation de la version 1.4 de l'outil AXIS présente un problème connu. Pour de plus amples renseignements, reportez-vous aux *Notes de parution*.

1. Générez les classes stubs à l'aide de WSDL2Java de l'outil AXIS. Pour de plus amples renseignements, consultez la section relative à la génération de classes de stubs à l'aide de WSDL2Java de l'outil AXIS dans le fichier PKI_loginServiceManaged_JAVA_steps. Recherchez le fichier dans l'emplacement suivant :

   ```
   $NX_ROOT/samples/sdk/websvc/java/test1_pki
   ```

2. Démarrez le service CA SDM.
3. Exécutez pdm_pki -p DEFAULT.

   DEFAULT.p12 est créé dans le répertoire actuel. Cette politique dispose d'un mot de passe similaire à son nom de politique (dans ce cas, DEFAULT).

   Remarque : Cette commande ajoute également la clé publique du certificat dans le champ pub_key (attribut public_key) de la table/de l'objet sapolicy.

4. Connectez-vous à CA SDM.
5. Sélectionnez Politique de services Web SOAP, Politiques sous l'onglet Administration.

   La page Liste des politiques d'accès aux services Web SOAP s'affiche.

6. Cliquez sur DEFAULT.

   La page Détail de la politique d'accès aux services Web SOAP s'ouvre.

7. Remplissez le champ Contact mandataire (dans cet exemple, ServiceDesk) et assurez-vous que le champ Avec clé de l'enregistrement de la politique PAR DÉFAUT indique Oui.
8. Copiez le fichier DEFAULT.p12 (à partir du répertoire dans lequel la commande pdm_pki est exécutée), le fichier JSP portant le nom *pkilogin.jsp* et le fichier HTML portant le nom *pkilogin.htm* (à partir du répertoire $NX_ROOT\samples\sdk\websvc\java\test1_pki) dans le répertoire suivant :

   ```
   $NX_ROOT/bopcfg/www/CATALINA_BASE/webapps/axis
   ```

9. Ouvrez le formulaire HTML à partir du répertoire axis. Par exemple, http://hôte_local:8080/axis/pkilogin.htm.

   Renseignez les champs appropriés.

   Remarque : Le champ Répertoire identifie l'emplacement du fichier de certificat. Définissez le chemin d'accès sur l'emplacement correct.

10. Cliquez sur Log me in!

    La page de résultats s'ouvre.

11. Cliquez sur l'URL BOPSID.

    Important : Cliquez immédiatement sur l'URL ! BOPSID dispose d'un jeton d'une durée limitée à environ 30 secondes.

    Le format d'une URL utilisant BOPSID est :

    http://<nom_serveur>:<port>/CAisd/pdmweb.exe?BOPSID=<valeur BOPSID>

Remarque : Pour utiliser la méthode loginServiceManaged pour un programme client Java s'exécutant sous AIX, vous devrez peut-être remplacer deux fichiers de politique de sécurité dans JAVA_HOME. Rendez-vous à l'adresse http://www.ibm.com et recherchez "developerworks java technology security information AIX". Dans le document "developerWorks, Java technology, Security", suivez le lien vers "IBM SDK Policy files". Téléchargez les fichiers de politique autorisés local_policy.jar et US_export_policy.jar. Utilisez ces fichiers pour remplacer les fichiers d'origine dans votre répertoire JAVA_HOME/lib/security.

Configuration de l’authentification PKI

Pour configurer l’authentification PKI, vous devez tout d’abord créer une politique d'accès. Voici la procédure à suivre :

Création d’une politique d'accès

L'administrateur effectue cette tâche à l'aide du produit (interface Web uniquement). Il doit également, comme cela est défini dans le processus, affecter un code texte unique à chaque stratégie d'accès.

Obtention d’un certificat numérique avec un couple de clés privées/publiques et association de ce certificat numérique à la politique d'accès

Pour procéder à l’authentification d’accès PKI, une application utilisateur doit obtenir un certificat numérique contenant à la fois un couple de clés publiques et un couple de clés privées. L’administrateur peut obtenir ce certificat numérique par l'entremise d'une autorité de certification tierce (CA) ou par le biais des produits de sécurité qui prennent en charge des certificats numériques. CA SDM propose également un utilitaire côté serveur capable de générer un certificat numérique. Il se situe dans le répertoire <NX_ROOT>/bin comme suit :

```
pdm_pki –p policy_code [–l certificate file] [–f] [-h]
```

-p

Identifie un code de stratégie unique.

-f

Permet à l'utilitaire de remplacer la clé publique existante par une nouvelle clé publique.

-l

Charge la clé publique stockée dans un certificat X509 V3.

-h

Affiche de l'aide sur la fenêtre de ligne de commande.

Si vous obtenez un certificat numérique par l'entremise d'un tiers, de CA Technologies ou de produits de sécurité, importez-le vers le même emplacement que le serveur CA SDM, puis associez-le à une politique d'accès. L’administrateur de l’application utilisateur obtient alors un fichier de certificat numérique incluant le contenu d’un certificat X509 V3 au format ASN.1/DER.

De plus, le certificat doit comporter uniquement la clé publique du couple de clés publique/privée. L’administrateur doit appeler l’utilitaire pdm_pki à l’aide de l’option –l pour charger le certificat. L’utilitaire charge ensuite le certificat, extrait la clé publique, convertit la clé publique au format texte BASE64 et l’enregistre avec une règle spécifiée par le code de la règle.

Lorsqu'un certificat numérique est généré à l'aide de l'utilitaire pdm_pki, l'administrateur appelle la commande dans CA SDM sans l'option -l. L'utilitaire génère ensuite un couple de clés privée/publique (il s'agit des clés RSA à 1 024 bits). La clé publique est convertie au format texte BASE64 et est stockée avec la politique d'accès spécifiée par le code de la règle. Un certificat X509 V3 est également créé pour conserver la clé publique avec d'autres informations (la phase de réussite par défaut est définie comme code de la règle). Enfin, le certificat X509 V3 est compilé avec la clé privée dans un format de certificat portable standard de PKCS12. Il est alors enregistré dans un fichier nommé *code_politique*.p12, en fonction du code de politique fourni. Ce fichier peut être exporté vers des clients.

Remarque : Si une politique d'accès a déjà été associée à la clé publique d'un certificat, les utilisateurs doivent spécifier l'option –f lorsqu'ils appellent la commande pdm_pki afin de remplacer la clé publique existante par une nouvelle clé publique.

Informations complémentaires :

Définition d'une politique d'accès (page 587)

Connexion aux services Web

Le tableau ci-dessous décrit le processus de connexion aux services Web configurés avec l'authentification PKI.

Processus	description
Chargement du certificat numérique et extraction de la clé privée	Le certificat numérique doit être stocké à un emplacement sécurisé du côté utilisateur, d'où il peut être extrait et utilisé pour la connexion aux services Web. Exemples de stockages sécurisés : ■ Magasin de certificats Windows ■ Magasin de certificats Java (géré par l'utilitaire java_keytool) ■ Annuaire de certificats (créé par les produits de sécurité d'autres CA Technologies). Une application utilisateur doit être capable de charger le certificat numérique et d'extraire la clé privée à l'aide des API appropriées, en fonction des environnements utilisateur.

Processus	description
Création d’une signature numérique du code de règle en texte brut avec la clé privée	Une fois la clé privée extraite du certificat numérique, elle peut être utilisée afin de générer une signature numérique pour le code de politique. La création d’une signature numérique permet de crypter le prétraitement d’un texte à l’aide d’une clé privée. L’algorithme de prétraitement doit être de type SHA1 standard et l’algorithme de cryptage, de type RSA. La signature numérique binaire doit également être convertie au format texte BASE64 avant son utilisation pour la connexion aux services Web. Selon les environnements utilisateur, les appels de l’API appropriés doivent être utilisés pour archiver ces informations.
Appel du service Web	Une application utilisateur doit appeler la méthode loginServiceManaged() des services Web, ainsi que le code de la règle en texte brut et la signature numérique au format texte BASE64 du code de règle.
Obtention de l’ID de session renvoyé	Si la demande d’accès est authentifiée, un ID de session en texte brut est automatiquement renvoyé.

Une fois l'ID de session généré, il établit une liaison entre une session de service Web et une politique d'accès. L'application utilisateur peut appeler d'autres méthodes de services Web avec cet ID de session. Ainsi, tous ses accès aux services Web sont contrôlés et gérés par cette politique d'accès.

Session et autorisation

Une validation réussie renvoie un ID de session associé au nom d’utilisateur validé, qu’il s’agisse du nom d’utilisateur fourni pour la connexion ou du contact mandataire spécifié dans une règle. Du fait de ce processus, chaque utilisateur de CA SDM se voit attribuer les droits de sécurité que vous voulez appliquer à votre application de service Web.

Par exemple, un utilisateur spécifique peut disposer d'une partition de données limitant les demandes visibles. Lorsqu'un utilisateur utilise un ID de session pour obtenir des informations sur les appels, le système CA SDM s'assure que la partition de données est appliquée.

La sécurité du groupe de fonctions est également appliquée. Par exemple, un utilisateur peut ne pas avoir accès au groupe de fonctions Call Manager. L'appel de méthodes de services Web (telles que l'affichage et la création de demandes) est rejeté, car l'accès est refusé au groupe de fonctions Call Manager.

Lorsque l'application a terminé la tâche qu'elle effectue pour un utilisateur, celui-ci doit appeler la méthode Logout() pour invalider l'ID de session.

Chaque ID de session arrive à expiration après une certaine période d'inactivité. Un ID de session arrive donc à expiration si l'intervalle de temps entre les appels de méthode dépasse un certain délai. Ce délai est défini dans le Gestionnaire d'options. Il est spécifié par l'option CA SDM suivante :

```
'webservice_session_timeout'
```

Si cette valeur est définie sur zéro (0), les ID de session n'arrivent jamais à expiration. Si cette option est manquante ou n'est pas définie, le délai est fixé par défaut à une heure. Si une méthode de service Web est appelée par l'entremise d'un ID de session expiré, une erreur est renvoyée avec le code d'erreur UDS_SESSION_TIMEOUT lors de son premier référencement, et UDS_BAD_SESSION par la suite.

Pour qu'un ID de session reste actif, appelez une méthode de service Web, quelle qu'elle soit, avant l'expiration du délai. Pour que l'ID de session reste actif si vous n'utilisez pas le serveur, appelez serverStatus().

Gestion et contrôle d'accès

Pour minimiser le problème potentiel que peut représenter la saturation de billets des services Web et pour maintenir la stabilité du serveur CA SDM, cette version des services Web de CA SDM utilise un système de gestion et de contrôle d'accès. Ce système a pour objectif principal de traiter le surplus d'activités de service lancées par des applications utilisateur approuvées et qui risquent de provoquer des exceptions ou des erreurs de programmation. Il sert également de barrière de protection des services web de CA SDM contre les attaques hostiles. L'administrateur d'une application de service Web peut créer et définir une politique d'accès dans CA SDM qui contrôle l'accès aux services Web de CA SDM à partir d'une application de service Web.

Remarque : Une politique d'accès par défaut avec un code DEFAULT est fournie. La politique d'accès par défaut ne comporte aucune restriction d'accès et s'applique uniquement aux sessions authentifiées par le biais d'un nom d'utilisateur et d'un mot de passe.

Définition d'une politique d'accès

Pour créer une politique d'accès aux services Web SOAP, un administrateur doit définir une politique d'accès.

Pour définir la politique d'accès :

1. Cliquez sur l'onglet Administration.
2. Dans l'arborescence située à gauche, cliquez sur Politique des services Web SOAP, Politiques.

   La page Liste des politiques d'accès aux services Web SOAP s'affiche.
3. Cliquez sur Créer.

   La boîte de dialogue Créer une politique d'accès aux services Web SOAP s'affiche.
4. Entrez les informations de la nouvelle politique d'accès :

   Remarque : La valeur par défaut -1 pour ce type d'opération indique qu'aucune restriction ne s'applique à l'opération correspondante Une valeur de 0 (zéro) indique que l'opération correspondante n'est pas autorisée.

   Symbole

   (Obligatoire) Identifie le nom symbolique d'une politique d'accès.

   Code

   (Obligatoire) Indique le texte unique qui identifie cette politique d'accès.

   Etat

   (Obligatoire) Identifie l'état d'une politique d'accès. Une politique inactive n'est pas utilisée.

   Contact mandataire

   Identifie le contact à utiliser pour toutes les opérations de services Web et pour la sécurité de CA SDM.

   Par défaut

   Identifie la politique par défaut. Définit cette règle en tant que politique par défaut. Une seule politique par défaut active est autorisée. La création d'une politique par défaut définit la politique par défaut actuelle sur un autre état que politique par défaut.

   Dispose d'une clé

   (Lecture seule) Indique si une clé publique a été associée à cette politique. Ce champ est mis à jour lorsqu'une clé publique est associée à une politique par le biais de l'utilitaire pdm_pki.

Autoriser représentant

Identifie l'autorisation d'emprunt d'identité. Si ce champ est défini, le souscripteur peut appeler la méthode de services Web impersonate() et créer une session de services Web au nom de l'utilisateur dont l'identité est à emprunter. L'authentification d'un accès supplémentaire n'est pas effectuée lors de la création de la session. Toutefois, cette méthode peut être appelée avec succès uniquement si la valeur access_level du type d'accès du nouvel utilisateur est inférieure ou égale à la valeur grant_level du type d'accès mandataire de l'utilisateur.

description

Indique la description détaillée de cette politique d'accès.

Création de tickets

Indique le nombre d'opérations d'insertion d'un ticket (appel, demande de changement et demande client) autorisées par heure.

Création d'objets

Indique le nombre d'opérations d'insertion d'un objet CA SDM (autre qu'un ticket) autorisées par heure.

Mises à jours d'objets

Indique le nombre d'opérations de mises à jour d'un objet CA SDM autorisées par heure.

Pièces jointes

Indique le nombre d'opérations sur les pièces jointes autorisées par heure.

Requêtes de données

Indique le nombre d'opérations de requêtes de données autorisées par heure.

Connaissances

Indique le nombre d'opérations sur les bases de connaissances autorisées par heure.

5. Cliquez sur Enregistrer.

   La politique de services Web SOAP est définie.

Méthodes de services Web par catégorie

Chaque méthode de services Web de CA SDM appartient à une catégorie précise. La liste suivante présente toutes les catégories et les méthodes qui leur sont associées :

Création de tickets

- createTicket()
- createQuickTicket ()

- createRequest()
- createChangeOrder()
- createIssue()

Création d'objets

- logComment()
- createAsset()
- addAssetLog()
- createAssetParentChildRelationship()
- createObject()
- createWorkFlowTask()
- createActivityLog()
- notifyContacts()
- addBookmark()
- addComment()
- createFolder()

Mises à jours d'objets

- addMemberToGroup()
- removeMemberFromGroup()
- closeTicket()
- createLrelRelationships()
- removeLrelRelationships()
- deleteWorkFlowTask()
- updateObject()
- transfer()
- escalate()
- attachChangeToRequest()
- detachChangeFromRequest()
- changeStatus()
- clearNotification()
- updateLrel()
- deleteBookmark()
- updateRating()

Pièces jointes

- createAttmnt()
- createAttachment()
- attachURLLink()
- deleteAttmnt()
- deleteComment()
- removeAttachment()

Requêtes de données

- impersonate()
- serverStatus()
- getBopsid()
- getConfigurationMode()
- getHandleForUserid()
- getAccessTypeForContact()
- getPermissionsGroup
- getObjectTypeInformation()
- getRelatedList()
- getRelatedListValues()
- getGroupMemberListValues()
- getPendingChangeTasksForContact()
- getPendingIssueTasksForContact()
- getWorkFlowTemplates()
- getWorkflowTemplateList()
- getTasksListValues()
- getNotificationsForContact()
- getPolicyInfo()
- getAssetExtensionInformation()
- getLrelValues()
- getObjectValues()
- doSelect()
- doQuery()
- getPropertyInfoForCategory()

- getValidTaskTransitions()
- getListValues()
- getListInfo()
- findContact()
- getAttmntInfo()
- getAttmntList()
- getBookmarks()
- getCategory()
- getComments()
- getContact()
- getDecisionTrees()
- getDocument()
- getDocumentTypes()
- getFolderInfo()
- getFolderList()
- getLrelLength()
- getPriorities()
- getRepositoryInfo()
- getStatuses()
- getTemplateList()

Connaissances

- createDocument()
- deleteDocument()
- doSelectKD()
- faq()
- attmntFolderLinkCount()
- getAttmntListPerKD()
- isAttmntLinkedKD()
- getDocumentByIDs()
- getKDListPerAttmnt()
- getQuestionsAsked()

- modifyDocument()
- rateDocument()
- search()

Lorsqu'une politique d'accès est mise à jour par CA SDM, les services Web mettent à jour les informations de règle correspondantes de manière dynamique. Les sessions actives de services Web répondant à cette politique restent contrôlées selon les configurations de cette règle. Les nouvelles sessions de services Web que cette politique doit gérer et contrôler doivent être conformes aux configurations les plus récentes.

Remarque : Pour plus d'informations au sujet de chaque méthode, reportez-vous au *Manuel de référence technique de CA SDM*.

Définition d'un type d'erreur

Des *types d'erreurs* sont affectés lors de la création de tickets et une politique d'accès définit un ensemble de ces types d'erreurs. Une application utilisateur des services Web de CA SDM peut utiliser des méthodes Web de bas niveau pour créer un ticket (demande, demande de changement ou demande client) en spécifiant un type d'erreur afin de classer l'erreur signalée par le ticket dans une catégorie. Les types d'erreur peuvent être utilisés uniquement en association avec la méthode de haut niveau createTicket(). Les méthodes de bas niveau, comme createRequest(), n'utilisent pas de types d'erreur.

Informations complémentaires :

Accès simplifié aux services Web (page 595)

Types d'erreurs des services Web

Les services Web CA SDM proposent également un ensemble défini de types d'erreurs par défaut, qui sont créés pour *chaque* politique. Ces types par défaut, appelés types d'erreurs *internes*, peuvent être désactivés, mais il est impossible de les supprimer. Dans le produit, vous pouvez utiliser la page Détail de la politique d'accès aux services Web pour voir les types d'erreurs par défaut qui sont fournis lorsqu'une nouvelle politique est créée.

Les informations ci-dessous décrivent chaque type d'erreur interne :

ACCESS_ERROR

Indique que le système n'a pas réussi à trouver ou à se connecter à une ressource (fichier, site Web, etc.).

EXCEPTION_FATAL

Indique que l'application s'arrête de manière inattendue.

EXCEPTION_RUNTIME

Indique que le code de l'application a détecté une exception.

LOGIN_ERROR

Indique que l'opérateur n'a pas réussi à accéder à l'application.

Types d'erreurs supplémentaires

L'administrateur d'une politique d'accès peut ajouter des types d'erreurs supplémentaires selon la méthode décrite ci-après :

Type d'erreur	description
Modèle de ticket	Identifie un modèle d'incident, d'erreur, de problème ou demande de changement utilisé pour créer un ticket lorsque ce type de problème est signalé. **Remarque :** Le contact de la politique propriétaire est utilisé comme utilisateur final. Les valeurs Type de ticket et Nom du modèle de ticket définissent le modèle de ticket.
Par défaut	Indique si ce type de problème est défini par défaut pour la politique. Un seul type par défaut est autorisé pour chaque règle. **Remarque :** Un nouveau type d'erreur par défaut remplace le type d'erreur par défaut associé à la politique.
Actif	Représente un type d'erreur actif. **Remarque :** Un type inactif ne crée pas de tickets.
Interne	Identifie le champ comme étant en lecture seule, ce qui indique s'il s'agit d'un type d'erreur interne, par défaut.
Symbole	Indique le nom symbolique du type d'erreur.
Code	Définit l'identificateur de texte unique du type d'erreur.
description	Décrit en détail le type d'erreur.
Gestion des doublons	Définit la procédure à suivre lorsque le produit détecte un ticket identique.

Type d'erreur	description
Renvoi des données	Identifie le message défini par l'utilisateur qui est renvoyé aux applications clientes par la méthode Web createTicket(). Renvoyer les données peut servir à indiquer une procédure que l'application devrait suivre (Renvoi des données d'application) ou un message (Renvoi des données de l'utilisateur) à afficher pour l'utilisateur final.

Informations complémentaires :

Gestion des tickets en double (page 594)

Gestion des tickets en double

La politique d'accès aux services Web peut détecter et gérer des tickets en double afin notamment d'empêcher l'inondation de tickets. Un ticket susceptible d'être dupliqué lors de sa création s'applique dans les cas suivants :

- Au moins un ticket de même type (demande, demande client ou demande de changement) existe déjà, et il est ACTIF.
- Le ticket existant a été créé par le service Web.
- Le ticket existant a été créé avec la même politique et le même type d'erreur que le ticket en cours de création.
- La date de création du ticket existant n'excède pas un seuil spécifié (par exemple, il est ouvert depuis moins de 2 jours).

  Remarque : Le champ de la date de création est configuré à l'aide de l'intervalle maximal pour la recherche des doublons.
- L'ID dupliqué correspond à celui fourni par les utilisateurs lorsqu'ils appellent la méthode createTicket().

Les utilisateurs peuvent également éviter l'existence des doublons en classant les tickets selon des critères personnalisés qui définissent les tickets comme uniques ou différents. Pour ce faire, ajoutez un paramètre de chaîne facultatif à l'appel des services Web createTicket. Si la gestion des doublons est activée, le paramètre de chaîne est contrôlé, une fois les autres critères de gestion des doublons vérifiés, pour déterminer s'il s'agit d'un appel unique ou d'un appel dupliqué de cette méthode.

Dupliquer les résultats de ticket

Si le ticket en cours de création est en fait un ticket dupliqué, le type d'erreur existant peut être configuré pour effectuer l'une des opérations suivantes :

Type d'erreur reconfiguré	Résultats
Créer le ticket et ignorer les doublons	Un nouveau numéro et un nouveau descripteur de ticket sont renvoyés (par défaut).
Ne pas créer de ticket ; Ajouter un journal d'activité au doublon existant	Le descripteur du ticket et le numéro du ticket existant sont renvoyés.
Ne pas créer de ticket ; Ajouter une entrée au journal standard de CA SDM	Un descripteur de ticket et un numéro de ticket existant sont renvoyés.
Créer un ticket et le joindre en tant qu'enfant au doublon	Un nouveau numéro et un nouveau descripteur de ticket sont renvoyés.

Accès simplifié aux services Web

Les services Web de CA SDM proposent une version abrégée de méthodes Services Web de haut niveau qui sont des versions simplifiées de méthodes Services Web existantes. La plupart des applications utilisateur n'ont pas besoin de disposer d'un large éventail de méthodes Services Web pour faire appel à des services de centre de service par le biais des services Web de CA SDM. Cet ensemble de méthodes de services Web de haut niveau, qui a recours aux politiques d'accès définies par l'utilisateur et aux paramètres par défaut définis dans les politiques, est capable de fonctionner avec une connaissance limitée du schéma d'objet de CA SDM. En outre, les méthodes de haut niveau couvrent un ensemble commun de fonctionnalités de CA SDM dont la plupart des applications orientées service ont besoin.

Voici comment utiliser ces méthodes de services Web de haut niveau :

createTicket (SID, Description, Error_Type, Userid, Asset, DuplicationID)

Vous devez indiquer un type d'erreur concernant l'erreur rapportée si vous utilisez cette méthode. Le type d'erreur doit contenir le modèle de ticket correspondant au ticket que vous souhaitez créer. Il doit définir la procédure à suivre en cas de ticket en double, spécifier les sorties de données et, enfin, être associé à la politique d'accès définie pour l'application utilisateur.

Lorsque cette méthode est appelée, les services Web de CA SDM localisent la politique d'accès en cours ainsi que le type d'erreur requis pour la création du ticket. Voici la méthode utilisée par les services Web de CA SDM pour localiser le type d'erreur correct :

- Si le code d'un type d'erreur spécifique est fourni dans les données d'entrée et qu'il correspond à un type d'erreur associé à la politique, ce type de problème est utilisé, qu'il soit interne ou non.

- Si aucun type d'erreur n'est spécifié ou qu'aucun type d'erreur n'a pu être localisé à l'étape précédente, le type d'erreur par défaut est utilisé s'il en existe un pour la politique.
- Si aucun type d'erreur par défaut n'a été défini pour la politique ou si l'étape précédente a échoué, le type d'erreur par défaut défini pour les problèmes internes est utilisé.

Une fois qu'un type d'erreur a été défini, les services Web de CA SDM s'en servent pour créer un ticket. L'utilisateur mandataire défini dans la politique d'accès est utilisé pour la création de ticket si l'ID d'utilisateur est vide et que les informations sur les actifs sont ajoutées au ticket (si l'entrée n'est pas vide). Après la création du ticket, les services Web de CA SDM renvoient les données utilisateur et les données d'application, comme indiqué par le type d'erreur.

closeTicket (SID, Description, TicketHandle)

Les utilisateurs peuvent appeler cette fonction pour fermer un ticket. Elle définit simplement l'état d'un ticket ouvert sur fermé et ajoute la description des données d'entrée au journal d'activité.

logComment (SID, TicketHandle, Comment, Internal_Flag)

Ajoute une entrée avec les commentaires des données d'entrée au journal d'activité du ticket ouvert.

getPolicyInfo (SID)

Permet aux utilisateurs d'obtenir des informations relatives à la politique qui contrôle la session de services Web en cours. Vous pouvez utiliser ces informations pour indiquer la capacité du serveur pour cette application utilisateur. Les utilisateurs peuvent ainsi ajuster leurs appels de services Web selon la capacité du serveur.

Grâce à cet ensemble d'API de services Web simplifiées, la plupart des utilisateurs n'ont pas à faire l'effort d'assimiler l'ensemble des API de services Web ainsi que le schéma de CA SDM. L'utilisation de cet ensemble simplifie et accélère le processus de création d'applications compatibles avec la technologie orientée services pour les utilisateurs.

Objets

CA SDM traite chaque entité (par exemple, un contact ou un problème) comme un *objet*. Ces objets de haut niveau sont définis dans les fichiers majic (.maj) et mod (.mod) sur le serveur CA SDM dans le répertoire suivant :

```
/bopcfg/majic
```

Les objets personnalisés sont définis dans le répertoire suivant :

```
/site/mods/majic
```

Les objets sont principalement des enveloppes de haut niveau autour d'une table de la base de données.

Le type d'objet (parfois appelé *sous-objet*) définit l'objet. Par exemple, les objets demande font partie du type Appel. Chaque type d'objet est défini par la déclaration OBJECT d'un fichier majic.

Remarque : Tous les objets fournis avec CA SDM sont répertoriés dans le Manuel de référence technique de CA SDM.

Un objet possède des *attributs*, lesquels correspondent essentiellement aux colonnes d'une table de base de données (à ne pas confondre avec les attributs XML). Les services Web proposent de nombreuses méthodes d'extraction des valeurs des attributs. De nombreuses méthodes exigent que vous nommiez les attributs afin de définir ou d'extraire des valeurs. Vous devez utiliser le nom de l'attribut assigné dans le fichier majic ou le fichier mod qui définit l'objet : celui-ci peut différer du nom actuel de la base de données. Les sites clients peuvent ajouter des attributs supplémentaires lors d'une personnalisation.

Remarque : Pour obtenir une liste de tous les attributs pour chaque objet, reportez-vous au *Manuel de référence technique de CA SDM*.

Les services Web identifient uniquement un objet par son *descripteur*, à savoir une valeur de chaîne de type *Typeobjet:ID*, *Typeobjet* correspondant au nom du type d'objet (sous-objet), et ID à une valeur unique. La valeur ID correspond à celle de l'attribut id présent pour chaque objet de CA SDM. Comme l'attribut id est presque toujours indexé dans le SGBD (Système de Gestion de Base de Données), l'utilisation de la portion ID du descripteur de l'objet est particulièrement utile pour la formulation de requêtes efficaces. Chaque objet, quel que soit son type, stocke cette valeur dans un attribut d'objet nommé persistent_id.

Remarque : Dans les versions précédentes, la partie ID du descripteur était toujours représentée par une chaîne de nombres entiers. Dans Unicenter Service Desk version r11.0 et ultérieure, la portion ID peut aussi être la représentation d'un UUID sous forme de chaîne, en général de 32 caractères.

La section ci-dessous répertorie les noms d'objet et les noms des sous-objets des entités qui utilisent les UUID.

de configuration	Nom du sous-objet
Contact	cnt
Actif	nr
Organisation	Organisation
Emplacement	Loc.
Entreprise/Fournisseur	ca_cmpny
Modèle	mfrmod

Les descripteurs sont *persistants* ; un descripteur représentant un objet particulier est toujours unique pendant toute la durée de sa vie, même en cas de migrations de base de données. Les clients peuvent souhaiter profiter de cette persistance lorsqu'ils utilisent des objets plutôt statiques, comme Etat et Types de contacts.

Les descripteurs d'objets sont essentiels pour utiliser correctement les services Web de CA SDM. De nombreuses méthodes, notamment celles de mise à jour de données, nécessitent des descripteurs. La plupart des méthodes qui renvoient les données d'un objet comprennent également le descripteur de l'objet.

Mise en cache et mises à jour du système

Les services Web mettent les informations des types d'objets en cache. Les informations relatives au type ne sont pas mises en cache avant le premier référencement de ce type, produisant ainsi un léger délai.

Pour éviter tout retard du serveur ou de la mise en cache, vous pouvez exécuter un client initial pour activer les services Web et mettre les informations concernant le type d'objet le plus fréquent en cache. La manière la plus simple de mettre les informations concernant le type d'objet en cache est d'effectuer des appels répétés à GetObjectTypeInformation(). Les types d'objets à prendre en compte pour cette technique sont les suivants :

Type d'objet	Définition
cr	Demande
chg	Demande de changement
iss	Demande client
cnt	Contact

Type d’objet	Définition
nr	Actif
wf	CA Workflow (Demandes de changement)
iss_wf	CA Workflow (Problèmes)
prp	Propriété (pour les demandes de changement et les demandes client)
prptpl	Modèle de propriété (pour les demandes de changement et les demandes client)
cr_prp	Propriété de la demande
cr_prptpl	Modèle de propriété de demande

Ajoutez tous les autres types d’objets référencés par votre code client.

Catégories et propriétés

Les objets demande, demande de changement et demande client disposent tous d'un champ de catégorie, utilisé pour classer la nature du ticket. Une catégorie peut avoir zéro, un ou plusieurs objets de propriété joints au ticket lorsque la catégorie est assignée. Certains de ces objets peuvent être marqués comme *obligatoires* : une valeur doit donc être indiquée avant l'enregistrement du ticket (cela s'applique aux opérations de mise à jour et d'insertion).

Les services Web de CA SDM fournissent automatiquement les valeurs par défaut pour tout ticket créé avec les services Web. La valeur par défaut (actuellement "-") est obtenue à partir du catalogue de messages localisés de CA SDM.

Si vous devez définir des valeurs de propriétés lors de la création, vous avez le choix entre trois méthodes de création de tickets : createChangeOrder, createIssue et createRequest. Chacune de ces méthodes possède un paramètre permettant de transmettre des valeurs pour chaque propriété. Pour savoir quelles propriétés seront jointes, vous devez déterminer les propriétés associées à la catégorie que vous souhaitez assigner au ticket. La méthode la plus simple est getPropertyInfoForCategory().

Remarque : Pour plus d'informations sur la méthode getPropertyInfoForCategory(), reportez-vous au *Manuel de référence technique de CA SDM*.

Pour identifier les valeurs valides pour une propriété, recherchez d'abord la règle de validation de la propriété pour le modèle de propriété adapté. Pour cela, demandez l'attribut validation_rule lorsque vous appelez la méthode getPropertyInfoForCategory. Récupérez ensuite le type validation_type associé à cette règle. Si le type est dropdown, vous pouvez alors utiliser la méthode getRelatedList pour récupérer les valeurs associées à la règle, en utilisant l'attribut BREL values dans l'objet prpval_rule.

Remarque : Pour plus d'informations, reportez-vous au *Manuel de référence technique de CA SDM*.

Pour définir des valeurs de propriété après une mise à jour effectuée grâce à la méthode updateObject(), vous devez interroger la liste de propriétés une fois la mise à jour effectuée. Pour ce faire, utilisez la méthode getRelatedList().

La validation de valeurs de propriété par les méthodes de service Web n'est pas prise en charge actuellement. Si vous souhaitiez, par exemple, affecter des valeurs de propriété à une règle de validation avec un type de validation d'option déroulante, vous devriez écrire un code supplémentaire pour créer des valeurs de propriété tout en créant la règle de validation d'option déroulante. N'attachez pas une valeur de propriété à une règle de validation de case à cocher.

Remarque : Pour plus d'informations sur les règles de validation de propriétés, reportez-vous au *Manuel d'administration*. Pour plus d'informations sur la création de règles de validation de propriétés par le biais de l'interface CA SDM, reportez-vous à *l'Aide en ligne*.

Renvois d'objets XML

De nombreuses méthodes de services Web renvoient une représentation XML des objets CA SDM. Les services Web utilisent une structure XML standard commençant par l'élément racine suivant :

```
<UDSObject>
```

Le format de la représentation XML est décrit dans le tableau suivant :

Elément XML	Type	description
<UDSObject>	N/D	Identifie le nœud racine.
<Handle>	Chaîne	Identifie le descripteur de l'objet.
<Attributes>	Séquence	Identifie les valeurs de l'attribut. Il comporte zéro, un ou plusieurs éléments pour les valeurs d'attributs de l'objet.

Elément XML	Type	description
<*attrName0* DataType = *“typeEnum"*>	Chaîne	Identifie *AttrName0,* à savoir un nom d'attribut de l'objet tel qu'il est défini dans le fichier majic (.maj) ou mod (.mod) de CA SDM. Ce nom peut utiliser une notation par insertion de point, selon la méthode Web utilisée. La valeur de l'élément correspond à la valeur de l'attribut. Un élément vide indique qu'une valeur nulle/vide est associée à l'attribut de cet objet. L'attribut DataType est un nombre entier indiquant le type de données de l'attribut utilisé dans l'environnement CA SDM.

Par exemple, un appel à la méthode getObjectValues() peut renvoyer des informations similaires à celles indiquées ci-dessous.

```
<UDSObject>
        <Handle>cnt:555A043EDDB36D4F97524F2496B35E75</Handle>
        <Attributes>
                <Attribute DataType="2003">
                        <AttrName>prénom</AttrName>
                        <AttrValue>prénom</AttrValue>
                        <DisplayValue>Yaakov</DisplayValue>
                </Attribute>
                <Attribute DataType="2005">
                        <AttrName>organisation</AttrName>
                                <AttrValue>342</AttrValue>
                <DisplayValue>Service Comptabilité</DisplayValue>
        </Attribute>
</Attributes>
        <Lists>         <List name="mylist1">
                        <UDSObject>...</UDSObject>
                        <UDSObject>...</UDSObject>
                </List>
        </Lists>
</UDSObject>
```

Certaines méthodes, telles que doSelect(), renvoient une séquence d'éléments <UDSObject> contenus dans un élément <UDSObjectList>.

La section <Lists> peut contenir aucun, un ou plusieurs noeuds <List>. Un noeud <List> contient aucun, un ou plusieurs noeuds <UDSObject>. En général, les éléments <List> sont renvoyés uniquement lorsqu'une requête spécifique pour les valeurs de la liste est effectuée.

Lorsque vous voulez renvoyer une liste de valeurs associées à un objet spécifique, il est conseillé d'utiliser la méthode *getRelatedListValues*.

Si une requête est effectuée uniquement pour une liste ne comportant pas de nom d'attribut, telle que actlog, l'élément <UDSObject> complet est renvoyé dans la section <List>.

Des méthodes spécialisées, telles que getDocument(), peuvent, bien sûr, être différentes. Lorsqu'une requête est effectuée pour un attribut, la valeur de la base de données est renvoyée. Pour les attributs SREL, cela n'est pas aussi utile. La requête de l'attribut du destinataire d'une demande renvoie un nombre entier car le REL_ATTR du contact (clé étrangère) correspond à son ID. Pour Unicenter Service Desk r11.0, les données renvoyées pour les attributs comprennent les éléments du SGBD (Système de Gestion de Base de Données) et la valeur de nom commune des références SREL.

méthodologie ITIL

Par défaut, les services Web prennent intégralement en charge la méthodologie ITIL. Les fonctionnalités ITIL de CA SDM vous permettent d'exploiter la méthodologie ITIL.

Création d'incident ou de problème

CA SDM prend en charge la méthodologie ITIL afin qu'il soit possible de créer des incidents et des problèmes à l'aide des services Web de CA SDM. Les incidents et les problèmes sont conservés dans l'objet cr (Call_Req). Son attribut de *type* signale l'enregistrement comme un incident, un problème ou une demande. Pour créer un incident, un problème ou une demande, appelez la méthode createRequest, puis indiquez la valeur correspondant à l'attribut de type.

L'attribut de type est un pointeur (SREL) vers l'objet crt (Call_Req_Type) : vous devez donc transférer un descripteur en tant que valeur.

Les exemples de code suivant illustrent la méthode de création d'un incident ou d'un problème en transférant le descripteur de l'objet crt correct à la méthode createRequest. La définition de l'attribut de *type* au sein de la paire nom-valeur transmise en tant que paramètre vers la méthode createRequest permet de créer les tickets suivants :

Exemple : Syntaxe d'un problème

```
attrVals = {"summary", "A new problem", "description", "new problem", "type",
"crt:181"}
USPSD.createRequest(SID, creatorHandle, attrVals, template, new String[0], new
String[0])
```

Exemple : Syntaxe d'un incident

```
attrVals = {"summary", "A new incident", "description", "new incident", "type",
"crt:182"}
USPSD.createRequest(SID, creatorHandle, attrVals, template, new String[0], new
String[0])
```

Informations complémentaires :

Descripteurs par défaut (page 606)

Requête pour les incidents ou les problèmes

Pour extraire les incidents ou les problèmes, incluez l'attribut de *type* de l'objet cr dans la clause WHERE. L'exemple suivant illustre une clause WHERE permettant d'extraire tous les incidents actifs. Cette clause WHERE peut être utilisée avec des méthodes qui effectuent des requêtes pour les objets cr, tels que doSelect et doQuery :

```
type.id = 182 AND active = 1
```

182 est une portion de l'ID du descripteur représentant les types d'incidents.

Remarque : Pour plus d'informations, reportez-vous au tableau des objets crt (Call_Req_Type) de la section Descripteurs par défaut (page 606). Pour plus d'informations sur la formulation de requêtes correctes, reportez-vous à la section Clause WHERE (page 368).

Attachement d'un incident à un problème

Vous pouvez associer un ou plusieurs incidents à un problème. L'attribut de problème d'un incident associe l'incident à un problème.

Exemple : Association d'un incident à un problème

Cet exemple illustre l'association un incident récemment créé à un problème existant.

Pour associer l'incident au problème et définir l'attribut de problème de l'incident, utilisez UpdateObject. Dans l'exemple de code suivant, l'attribut de problème est défini sur le descripteur du ticket d'un problème existant :

```
attributeValues = {“problem”, “cr:12346”}
USPSD.UpdateObject(SID, incidentHandle, attributeValues, new String [0])
```

Association d'un problème à une demande de changement

Les incidents et les problèmes peuvent être liés à des demandes de changement à l'aide de la méthode attachChangeToRequest. L'exemple de code suivant utilise cette méthode pour créer simultanément une demande de changement et l'associer au problème. Dans cet exemple, cr:12347 est le descripteur d'objet du problème : il transmet un descripteur vide pour le quatrième paramètre, ce qui implique la création d'un changement par la méthode :

```
UPSPSD.attachChangeToRequest(SID, creatorHandle, "cr:12347", "", new String[0],
"activity description")
```

Eléments de configuration

La méthodologie ITIL emploie l'expression *Elément de configuration* (CI) pour désigner les logiciels, le matériel et les autres ressources informatiques. Cette expression fait référence à l'objet nr stocké dans la table de la base de données CA Technologies. Toutes les méthodes qui utilisent des objets d'*actif* utilisent aussi des CI. Il s'agit d'une simple différence de terminologie.

Utilisation des services Web

Cette section décrit les principes élémentaires d'utilisation des services Web de CA SDM. L'exemple de code illustrant l'utilisation des services Web se trouve dans les répertoires d'installation de CA SDM suivants :

```
<NX_ROOT>/samples/sdk/websvc/java
```

L'exemple de code présenté est écrit en langage Java et utilise Apache Axis pour la messagerie SOAP.

Connexions

Avant d'être en mesure d'utiliser une méthode Services Web, vous devez vous procurer un ID de session à partir de l'une des méthodes suivantes : login(), loginService() et loginServiceManaged(). Les deux premières méthodes nécessitent un nom d'utilisateur et un mot de passe validés exactement de la même manière que le client Web de CA SDM ; le type d'accès du contact spécifie la méthode de validation. La troisième méthode nécessite une paire de clés publique/privée, pour laquelle une demande de connexion cryptée à l'aide d'une clé privée ne peut être décryptée que grâce à la clé publique, et inversement.

Informations complémentaires :

Caractéristiques externes (page 577)

Exécution des tâches communes

Les services Web fournissent une API flexible et puissante dans CA SDM, mais leur utilisation nécessite une certaine connaissance de la structure d'objets utilisée par le produit :

1. Familiarisez-vous avec les informations sur les objets et les attributs fournies dans le *Manuel de référence technique*.

   Celui-ci répertorie les attributs de chaque objet du système ; il est indispensable de connaître ces attributs, car de nombreuses méthodes Services Web exigent le nom des attributs.

2. Vérifiez les méthodes de services Web, particulièrement les méthodes génériques. Par exemple, si votre application doit afficher tous les journaux d'activité d'un appel, identifiez d'abord le lien entre les journaux d'activité et l'appel.

   Le *Manuel de référence technique* indique que l'objet de demande contient deux listes de journaux d'activité : act_log (qui affiche uniquement les journaux non internes) et act_log_all (qui répertorie tous les journaux d'activité).

3. Identifiez les méthodes de services Web requises. Pour obtenir les listes jointes à un objet, utilisez la méthode getRelatedList() ou getRelatedListValues().

Descripteurs par défaut

Certaines données par défaut fournies par le produit sont souvent utilisées. Pour éviter d'avoir à rechercher les descripteurs correspondant à ces objets, certaines de ces données ont été répertoriées dans les tableaux ci-après.

Remarque : Bien que les descripteurs ne changent pas, les symboles lisibles peuvent être modifiés.

Type de contact (nom de l'objet : ctp)

Descripteur	Remarque
ctp:2307	Type Analyste
ctp:2310	Type Client
ctp:2305	Type Employé
ctp:2308	Type Groupe

Impact (nom de l'objet : imp)

Descripteur	Remarque
imp:1605	Impact Aucun
imp:1600	Impact bas 5
imp:1601	Impact moyen-bas 4
imp:1602	Impact moyen 3
imp 1603	Impact moyen-haut 2
imp:1604	Impact haut 1

Priorité (nom de l'objet : pri)

Descripteur	Remarque
pri:505	Priorité non affectée Aucune
pri:500	Priorité faible 5
pri:501	Priorité intermédiaire-faible 4
pri:502	Priorité intermédiaire 3
pri:503	Priorité intermédiaire-haute 2
pri:504	Priorité haute 1

Gravité (nom de l'objet : sev)

Descripteur	Remarque
sev:800	Gravité basse 1
sev:801	Gravité moyenne-basse 2
sev:802	Gravité moyenne 3
sev:803	Gravité moyenne-haute 4
sev:804	Gravité haute 5

Type d'appel (nom de l'objet : crt)

Descripteur	Remarque
crt:180	Demande
crt:181	Problème
crt:182	Incident

Requête par appels, demandes client ou demandes de changement assignée à un contact

L'extraction des demandes actives assignées à un analyste (destinataire) constitue l'une des opérations les plus courantes. Pour effectuer cette opération, vous pouvez utiliser différentes méthodes : la méthode doQuery()) permet d'obtenir une liste des références, la méthode doSelect() d'obtenir les valeurs immédiatement. Si le descripteur du destinataire est déjà connu, voici la clause WHERE à utiliser :

```
assignee.id = U'<assigneeID>' AND active = 1
```

Dans cette clause Where, <assigneeID> est la portion d'ID d'un descripteur de contact ou d'une valeur, telle que 555A043EDDB36D4F97524F2496B35E75.

Cette clause WHERE fonctionne pour les demandes, les demandes de changement et les demandes client, car ils comportent tous les attributs actifs (active) ou de destinataire (assignee) et ont la même signification pour les trois types d'objets. La portion active = 1 de la clause WHERE limite la recherche aux demandes actives.

Indicateur actif

La plupart des objets de CA SDM disposent d'un champ appelé active ou delete_flag. Il s'agit en fait d'un pointeur SREL vers l'objet Active_Boolean_Table ou Boolean_Table. Imaginons que vous ajoutez ces champs à vos requêtes afin de filtrer les objets marqués comme inactifs par l'administrateur système. Pour procéder à une requête, recherchez delete_flag = 0 pour localiser les enregistrements actifs, et delete_flag = 1 pour trouver les enregistrements inactifs. Ainsi, le pseudo-code suivant est un exemple d'utilisation de la méthode doSelect() pour extraire les valeurs de tous les objets Etat de la demande actifs :

```
doSelect(SID, "crs", "delete_flag = 0", -1, new String[0]);
```

Pour définir un objet comme actif ou inactif, vous devez transmettre le descripteur de l'objet booléen représentant la valeur Vrai ou Faux. Ces descripteurs ne changent pas : vous pouvez donc les coder en dur en toute sécurité. Ils sont énumérés ci-après.

Active_Boolean_Table	Boolean_Table
actbool:4551 = 'Active'	bool:200 = 'False'
actbool:4552 = 'Inactive'	bool:201 = 'True'

Extraction des longueurs de la liste associée

Lorsque vous appelez les valeurs d'attributs d'un objet, avec la méthode getObjectValues() par exemple, vous pouvez obtenir la longueur d'une liste associée en demandant l'attribut suivant :

```
<listName>.length
```

Ainsi, pour obtenir le nombre de journaux d'activité d'une certaine demande, transmettez l'attribut suivant à la méthode getObjectValues() :

```
act_log_all.length
```

Remarque : Il s'agit de la seule façon d'utiliser les noms de liste dans ces types de méthodes.

REST (Representational State Transfer) est un type d'architecture logicielle qui permet de concevoir des systèmes hypermédia distribués, comme le World Wide Web. L'API REST de CA SDM permet aux développeurs d'applications, d'intégrations et Web de compiler la compilation des interfaces utilisateurs et des applications pour des unités telles que des tablettes et des téléphones intelligents. Les utilisateurs tels que des analystes, des employés et des clients peuvent alors utiliser l'interface utilisateur ou l'application sur ces périphériques. Par exemple, les développeurs d'applications peuvent développer une interface utilisateur CA SDM qui permet aux analystes d'utiliser des périphériques pour mettre à jour des billets.

L'API REST accède aux ressources à l'aide d'un URI (Uniform Resource Identifier), à savoir une chaîne de caractères de URI qui identifie un nom ou une ressource sur Internet. Dans CA SDM, les ressources peuvent être des objets tels que des billets, des actifs, des contacts, etc. Une application utilisant l'API REST créé une requête HTTP pour un URI et analyse la réponse. Cette identification active l'interaction avec les représentations de la ressource dans un réseau. Chaque client à une demande du serveur contient toutes les informations nécessaires à sa compréhension et n'utilise aucun contexte stocké sur le serveur.

Les développeurs utilisent l'API REST pour envoyer directement des requêtes HTTP au serveur pour la ressource qu'ils veulent manipuler. Les développeurs ont uniquement besoin d'une bibliothèque client HTTP, disponible dans la plupart des langages de programmation. L'API REST étant basé sur des standards libres, vous pouvez utiliser un langage de programmation Java pour y accéder.

Remarque : Pour de plus amples renseignements sur les méthodes REST HTTP, reportez-vous au *Manuel de référence technique*.

REST et SOAP

CA SDM contient les API de services Web REST et SOAP. Le public visé par l'API REST est un client d'interface utilisateur, tandis que le public visé par l'API SOAP est un programme. Les services REST concernent des ressources (manipulation d'objets, modification d'états d'objet, échange de représentations et utilisation de noms au lieu de verbes). Les services SOAP concernent des services (appel de méthodes, utilisation de verbes et réalisation des actions).

REST fournit les avantages suivants sur SOAP :

- REST est léger, basé sur HTTP et sans état (pour la modularité).
- REST prend en charge l'ajout de signet et la mise en cache de clients.
- REST conserve librement le contrat de données.
- La consommation de REST par des technologies frontales telles que WEB 2.0 et AJAX, s'effectue de manière simple.
- REST prend en charge les formats XML et de données JSON.
- REST améliore les performances.

Sécurité REST

La sécurité utilise plusieurs mécanismes d'authentification, y compris une approche personnalisée qui utilise des clés secrètes partagées.

Le produit prend en charge les schémas d'authentification de sécurité suivants :

- Authentification de clé secrète de services Web REST (utilise SSL et HMAC pour la connexion)
- Authentification de base REST (efface le texte codé de nom d'utilisateur/mot de passe)
- Authentification BOPSID REST (valide les BOPSID de CA SDM)
- Authentification d'artefact externe (CA EEM) (jeton d'artefact CA EEM)

Fonctionnement de l'authentification de clé secrète

L'authentification de clé secrète CA SDM est un processus qui vérifie les éléments suivants :

- L'identité du demandeur
- Le demandeur est un utilisateur enregistré.

L'authentification de clé secrète requiert que chaque demande inclue des informations concernant l'identité du demandeur. La demande doit également inclure des informations supplémentaires que CA SDM peut utiliser pour vérifier l'authenticité de l'utilisateur. Lorsque la demande est transmise à ce test de vérification, elle est considérée comme authentique. Lors de l'authentification d'une demande de touche d'accès, l'authentification secrète CA SDM procède comme suit :

1. Affecte une touche d'accès à un client. La touche d'accès identifie le client responsable d'une demande et utilise l'ID de session CA SDM comme valeur de clé. Une touche d'accès étant envoyée comme paramètre de demande, elle n'est pas secrète. Chaque utilisateur envoyant une demande à CA SDM peut utiliser le paramètre de demande ; par conséquent, une clé secrète est nécessaire.

2. Une touche secrète est affectée. Une touche secrète est une séquence alphanumérique incluant 40 caractères de façon dynamique et générée par CA SDM pendant la connexion. Le produit chiffre cette touche secrète avant de la stocker dans la base de données.
3. Des informations fournies par les clients (signature de demande utilisant la touche secrète) sont utilisées pour identifier le client et vérifier que la demande est autorisée. Ces informations supplémentaires protègent les utilisateurs contre l'emprunt d'identité et illustrent la propriété d'un secret partagé connu uniquement de CA SDM et du demandeur.

Options du service Web

Ces options contrôlent la session du service Web :

rest_webservice_access_duration

Spécifie le nombre d'heures pendant lesquelles la touche d'accès aux services Web REST demeure active avant d'expirer. Le délai d'expiration de la touche d'accès ne dépend pas du temps d'inactivité, mais de la durée depuis la création de cette touche d'accès. Une fois que la touche d'accès correspond à la durée spécifiée, la touche d'accès finit expire, qu'elle soit utilisée ou non.

De même, le client REST peut également fournir la durée de la touche d'accès spécifique lors de la demande de touche d'accès. Pour fournir la valeur de durée, définissez-la directement dans l'attribut de expiration_date de la ressource de rest_access, dans le cadre de la charge utile de demande POST.

Plage valide : 1 à 8760 heures

Valeur par défaut : 168

rest_webservice_disable_basic_auth

Désactive l'authentification de base dans les services Web REST.

Valeur par défaut : Non

rest_webservice_list_max_length

Spécifie le nombre maximum de lignes renvoyées par une requête de service Web REST.

Valeur par défaut : 500

rest_webservice_list_page_length

Spécifie le nombre par défaut de lignes renvoyées par une requête de service Web REST par page.

Plage valide : 1 à 500

Valeur par défaut : 25

rest_webservice_resources_to_expose

Spécifie la liste de sous-objets Majic (ressources) exposés par CA SDM par l'entremise de services Web REST. Cette option remplace le comportement par défaut. Par défaut, CA SDM expose tous les sous-objets par l'entremise de services Web REST.

Si vous n'introduisez aucun valeur dans cette option, les sous-objet Majic qui n'ont pas de propriété REST_OPERATIONS définie sur Aucun seront exposés. Par défaut, aucun sous-objet Majic ne dispose de cette propriété définie sur Aucun.

Utilisez la propriété REST_OPERATIONS pour définir les méthodes HTTP CRUD spécifiques (création, lecture, mise à jour et suppression) de sorte que CA SDM expose un sous-objet Majic donné.

Valeur par défaut : rest_access

Exemple : rest_access, cnt, grp, cr, crs, pri, alg, urg, imp, pcat, org

hmac_algorithm

Spécifie l'algorithme que vous utilisez pour calculer la signature de l'authentification de clé personnalisée/secrète dans les services Web REST.

Valeur par défaut : HmacSHA1

string_to_sign_fields

Spécifie les champs que vous utilisez pour calculer la signature pour l'authentification de clé personnalisée/secrète dans les services Web REST, en plus des champs REQUEST_METHOD, REQUEST_URI et QUERY_STRING par défaut.

Valeur par défaut : vide

webservice_domsrvr

Indique le nom du moteur d'objets utilisé par les services Web SOAP. Si cette option n'est pas installée, les services Web SOAP utilisent domsrvr.

La valeur de cette option doit être une chaîne commençant par les caractères "domsrvr:".

webservice_session_timeout

Définit la valeur du délai d'expiration (en minutes) pour les sessions du service Web SOAP. Lorsque le délai entre les appels de méthode Web successifs est supérieur à la valeur spécifiée, l'ID de session est marqué comme expiré. La session n'est alors plus valide.

Pour éviter l'expiration de sessions en raison de l'activité, définissez la valeur de cette option sur 0. D'autres méthodes, telles que les routines de déconnexion, peuvent encore rendre des sessions non valides.

Remarque : Ces options requièrent le redémarrage du serveur CA SDM.

Chapitre 13: Intégration à d'autres produits

Vous pouvez intégrer CA SDM à certains produits CA Technologies, mais nous ne fournissons pas d'informations détaillées sur l'intégration à tous les produits CA Technologies.

Remarque : Pour de plus amples renseignements sur les intégrations supplémentaires à CA SDM non décrites dans cette section, reportez-vous au *Livre vert CA Unicenter Service Desk Integrations* à l'adresse http://www.ca.com/worldwide.

Ce chapitre traite des sujets suivants :

Intégration de CA Workflow (page 615)
Intégration CA Portal (page 620)
Intégration des produits d'ordinateur central (page 627)
Intégration de CA Business Service Insight (page 630)

Intégration de CA Workflow

Un flux de travaux (workflow) désigne les tâches, les procédures, les organisations ou les individus impliqués, les informations requises en entrée et en sortie, ainsi que les outils nécessaires à la gestion et au contrôle de chaque étape d'un processus commercial. Le service CA Workflow offre une solution complète de gestion des processus commerciaux.

En général, le terme *flux de travaux* (ou workflow) désigne l'automatisation intégrale ou partielle d'un processus commercial, pendant laquelle des documents, informations ou tâches sont transmises d'un participant à un autre en vue d'entreprendre l'action qui convient conformément à un ensemble de règles procédurales.

CA Workflow est un système générique de gestion des flux de travaux. Evolutif et hautement performant, il permet de définir, de gérer et d'exécuter des flux de travaux et offre une solution de « workflow » générique.

CA Workflow est intégré à CA SDM à l'aide des services Web.

Composants de CA Workflow

CA Workflow utilise les composants suivants fournis avec le Kit d'intégration de flux de travaux :

- CA Workflow Design Environment (page 616)
- Serveur Workflow (page 618)
- Liste de travail (page 618)

CA Workflow Design Environment

Utilisez CA Workflow Design Environment pour créer et gérer des flux de travaux. CA Workflow Design Environment constitue l'outil principal à l'aide duquel vous pouvez créer et gérer des définitions de processus et des instances de flux de travaux, mais aussi contrôler les relations entre les participants d'un flux de travaux.

Une entreprise crée un processus commercial afin d'identifier les ressources, les activités manuelles et automatisées ainsi que les relations entre les diverses activités pour atteindre ses objectifs commerciaux. Un flux de travaux permet d'automatiser tout ou partie du processus commercial en déterminant les activités qui y sont liées dans le cadre d'une définition de processus. Ces activités de flux de travaux impliquent souvent la transmission de formulaires, de tâches ou d'informations d'une ressource à une autre, qu'il s'agisse d'une personne ou d'un logiciel.

Une définition de processus est une représentation de votre processus commercial. Elle est constituée de nœuds, d'événements, de rôles, d'acteurs, de tâches et de critères qui accompagnent le processus du début à la fin.

Alors que les définitions de processus représentent ce que souhaitez voir se produire au cours de votre processus commercial, les instances de processus reflètent ce qui se produit réellement. En exécutant une définition de processus, vous créez une instance de processus. Vous pouvez créer plusieurs instances de processus pour une même définition de processus. On parle alors aussi d'instance de définition de processus.

Démarrage de CA Workflow Design Environment (Windows)

A tout moment, vous pouvez démarrer CA Workflow Design Environment (Windows) pour créer et gérer des flux de travaux. Pour démarrer CA Workflow Design Environment, sélectionnez Démarrer, Tous les programmes, CA, CA Service Desk, IDE CA Workflow.

Remarque : Vous pouvez également démarrer CA Workflow Design Environment en double-cliquant sur le fichier *ide.bat* situé dans le répertoire $NX_ROOT\site\Workflow\Client. Si le classpath de l'IDE exige des ajouts pour satisfaire la configuration requise pour l'application, vous devez modifier le paramètre APPCPATH dans le fichier ide.bat et recourir au fichier ide.bat pour appeler l'IDE.

Démarrage de CA Workflow Design Environment (Linux)

A tout moment, vous pouvez démarrer CA Workflow Design Environment (Windows) pour créer et gérer des flux de travaux. Pour démarrer CA Workflow Design Environment, exécutez le fichier *ide.sh* situé dans le répertoire $NX_ROOT/site/Workflow/Client. L'interface de l'IDE CA Workflow n'est pas prise en charge sous UNIX.

Remarque : Pour se conformer aux exigences des applications, le fichier ide.sh dispose d'un paramètre APPCPATH qui peut être modifié pour l'ajout à la variable classpath.

Paramètres de l'IDE CA Workflow

Lorsque vous accédez à CA Workflow Design Environment, un écran de connexion s'affiche. Cette fenêtre de connexion est pré-remplie avec le nom d'utilisateur, le mot de passe et la connexion URL. Pour bénéficier d'un accès simplifié à l'IDE, vous pouvez ignorer entièrement l'écran de connexion en utilisant une combinaison des paramètres de ligne de commande suivants :

```
-u <nom_utilisateur>
-p <mot_de_passe>
-url <URL PM>
-t <jeton SafeSession eIAM>
```

Vous avez la possibilité d'appeler l'IDE en fournissant soit un nom d'utilisateur et un mot de passe (-u et -p), soit un jeton (-t). Le jeton –t désigne une session SafeSession exportée (on utilise aussi le terme artefact), c'est-à-dire une chaîne. Des produits parents peuvent ainsi simplement réutiliser toutes les sessions SafeSession existantes dont ils peuvent disposer, sans avoir à demander à nouveau un nom d'utilisateur et un mot de passe.

Vous devez obligatoirement fournir le paramètre –url, que vous utilisiez la méthode ID d'utilisateur/mot de passe –u et –p ou bien la méthode du jeton –t.

Par exemple, [-u, -p, -url] ou [-t, -url].

Pour utiliser cette fonction et ignorer l'écran de connexion IDE, modifiez soit le fichier ide.bat (sous Microsoft Windows) ou le fichier ide.sh (sous Linux) pour ajouter ces paramètres à la liste des paramètres transmis à la commande Java.

Remarque : Vous ne pouvez pas utiliser cette fonction avec le fichier ide.exe.

serveur CA Workflow

Le serveur CA Workflow fournit des services de gestion et d'exécution des processus de flux de travaux. Il est formé de trois composants :

- Les adaptateurs d'acteurs : ils permettent d'étendre les fonctionnalités des activités de flux de travaux.
- Le moteur de processus : il est chargé d'exécuter les instances de définitions de processus.
- Le gestionnaire de processus : il permet de gérer les définitions et les instances de processus.

Tous les clients de flux de travaux, le concepteur de processus, la liste de travail et les API des services Web et Java font appel à des services fournis par le serveur Workflow.

Liste de travail

Vous pouvez lancer la liste de travail par l'entremise d'un navigateur Web (par exemple http://<*nom_hôte*>:<*numéro_port*>/wl) ou par le biais d'appels API à partir d'un produit d'intégration.

Accès à CA Workflow

CA SDM offre une gestion des flux de travaux grâce à un moteur commun de flux de travaux. Ce système de flux de travaux fournit un environnement de définition de flux de travaux graphique, des mécanismes de branchement sophistiqués et la possibilité d'interagir avec les personnes qui n'ont pas directement accès à l'application CA SDM pour l'obtention des approbations. Vous pouvez utiliser l'authentification de CA Workflow et ajouter des utilisateurs (page 619) aux groupes de CA Workflow.

CA EEM et CA Workflow

Toutes les connexions à CA Workflow sont authentifiées par CA EEM. L'utilisateur doit disposer d'un enregistrement d'utilisateur CA EEM pour accéder à l'IDE ou à l'application Worklist de CA Workflow. L'administrateur CA Workflow, spécifié lors de la configuration de CA SDM, bénéficie d'un accès complet à CA Workflow. Par défaut, CA SDM fait appel à cet administrateur pour l'intégration de CA Workflow. Le compte de cet utilisateur est défini par les options cawf_username et cawf_password du Gestionnaire d'options. Vous devez vous assurer que le nom d'utilisateur et le mot de passe définis sont corrects et que l'utilisateur dispose d'un accès complet aux ressources CA Workflow dans CA EEM.

Classes de ressources

CA Workflow utilise également CA EEM pour restreindre l'accès à certaines fonctions de CA Workflow. Deux classes de ressources permettent de contrôler l'accès :

IDE

La ressource IDE permet une seule action, dite de *connexion*, qui permet de se connecter à l'interface IDE. Pour se connecter à l'application IDE de CA Workflow, l'utilisateur doit être autorisé à exécuter cette action.

Processus

La ressource Processus permet une seule action, dite de *démarrage*, qui permet de démarrer une instance de processus. Pour démarrer des processus à partir de l'application Web Worklist, l'utilisateur doit être autorisé à exécuter cette action. Tous les utilisateurs ont accès à l'application de liste de travail CA Workflow pour afficher et exécuter des tâches d'élément de travail. Cette autorisation permet uniquement le démarrage de nouvelles instances à partir de l'application Worklist.

Remarque : Ces classes de ressources sont définies avec l'instance d'application CA SDM dans CA EEM. Lorsque vous vous connectez à l'interface utilisateur Web d'CA EEM, vous devez préciser l'instance de l'application CA SDM afin de voir les ressources, politiques et groupes présentés ici.

Ajout d'utilisateurs à des groupes CA Workflow

Les utilisateurs ayant besoin de se connecter à l'IDE ou de démarrer des instances de processus doivent bénéficier d'une autorisation pour les ressources et les deux actions associées. La configuration de CA SDM ajoute deux politiques à CA EEM donnant accès à ces ressources. Deux groupes d'utilisateurs se voient également accorder des droits sur les politiques : les administrateurs de CA Workflow et les initiateurs de processus de CA Workflow. L'ajout d'utilisateurs au groupe Administrateurs de CA Workflow leur donne accès à l'IDE. L'ajout d'utilisateurs au groupe Initiateurs des processus de CA Workflow permet à ces derniers de démarrer des processus à partir de l'application Worklist.

Pour ajouter/supprimer des utilisateurs des groupes sur l'ordinateur où CA EEM est installé

1. Effectuez l'une des opérations suivantes :
   - Pour CA EEM r8.4 SP4 CR05, sélectionnez Démarrer, Programmes, CA, Embedded Entitlements Manager, EEM UI.
   - Pour CA EEM r12 CR02, sélectionnez Démarrer, Programmes, CA, Embedded Entitlements Manager, Admin UI.

   La fenêtre de connexion s'affiche.
2. Sélectionnez l'application CA SDM et entrez nom et le mot de passe d'administrateur de CA EEM.

   La fenêtre CA EEM principale s'affiche.

3. Sélectionnez Gérer les identités.
4. Sélectionnez l'option de recherche d'utilisateurs, entrez les critères de recherche, puis cliquez sur Rechercher.
5. Sélectionnez un utilisateur dans la liste de résultats.
6. Dans les données détaillées de l'utilisateur, ajoutez ou supprimez l'appartenance à un groupe dans la section Application Group Membership (Appartenance à des groupes d'applications).

   Si cette section ne s'affiche pas, cliquez sur Ajouter les détails des utilisateurs de l'application.
7. Cliquez sur Enregistrer.

   Les utilisateurs sont ajoutés aux groupes.

Intégration CA Portal

Vous pouvez accéder à des composants de CA SDM par le biais de CA Management Portal et CA Portal.

Remarque : CA Management Portal et CA Portal ne sont pas fournis avec CA SDM. Vous devez les acheter séparément et ils disposent chacun d'une licence distincte. CA SDM fournit uniquement les informations de base pour accéder à CA SDM par l'entremise de la fonction d'administration de portail. Pour de plus amples renseignements, reportez-vous à l'*Aide en ligne de CA Portal et de CA Management Portal Server Administration*.

Vérification de l'accessibilité à l'interface Web CA SDM

Après avoir installé CA SDM sur un système, assurez-vous que vous pouvez accéder à l'interface Web par l'entremise du serveur Tomcat. Pour que l'intégration du portail puisse réussir, l'interface Web d'CA SDM doit être accessible par l'entremise du serveur Tomcat.

Remarque : Pour l'installation de CA SDM sur un serveur LINUX, vous devez définir LD_LIBRARY_PATH sur $NX_ROOT/sdk/lib.

Installation et démarrage de CA Portal

Pour plus d'informations sur l'installation, le démarrage et l'arrêt de CA Portal, reportez-vous au *Manuel de mise en oeuvre de CA Portal* qui s'applique à votre installation.

Remarque : Vous pouvez installer CA Portal sur le système sur lequel CA SDM est installé ou sur un système distinct.

Intégration de portlets

Vous pouvez utiliser le produit en incluant des portlets de CA SDM dans le portail.

Pour inclure des portlets

1. Connectez-vous à CA SDM et cliquez sur Rechercher dans le Gestionnaire d'options de l'onglet Administration.

   La fenêtre Liste des options s'affiche.

2. Cliquez sur Portal_Safe_List.

   La fenêtre Détail de Portal_Safe_List s'affiche.

3. Entrez *nom_serveur:numéro_port* à l'emplacement où le portail a été installé dans le champ Valeur de l'option.

   Remarque : Pour plus d'informations sur cette option, reportez-vous à l'*Aide en ligne*.

4. Cliquez sur Installer.

5. Redémarrez le démon CA SDM.

6. Connectez-vous à CA Portal en tant qu'administrateur.

7. Créez un utilisateur CA SDM valide. Pour plus d'informations sur la création d'un utilisateur, reportez-vous à la documentation de CA Portal.

   Remarque : Le mot de passe utilisé lors de la création de cet utilisateur dans le portail peut être différent du mot de passe utilisé par ce même utilisateur pour se connecter à CA SDM, puisque CA SDM authentifie les utilisateurs pour cette intégration à l'aide d'une combinaison alliant le nom d'utilisateur, une session CA Portal valide et la valeur d'installation de CA Portal, si disponible, dans l'option PORTAL_SAFE_LIST.

8. Sélectionnez Connaissances dans la barre de menus principale de CA Portal.

   La page Connaissances s'affiche.

9. Sélectionnez Bibliothèque dans la barre Connaissances du volet gauche.

   L'arborescence de la bibliothèque s'ouvre dans le volet gauche.

10. Sélectionnez (ou créez et sélectionnez, si nécessaire) un dossier dans l'arborescence de la bibliothèque, puis cliquez sur l'option de publication de fichier dans la barre Connaissances du volet droit.

    Le formulaire de publication du fichier s'ouvre.

11. Tapez l'URL de portlet CA SDM suivante dans la zone de texte Contenu de l'onglet Informations générales :

    ```
    http://nom_hôte:numéro_port/CAisd/PortalServlet?USERNAME=$USER.username$&PORTALSESSION=$SESSION$&PORTALINSTALL=nom_hôte_portail:numéro_port_portail
    ```

    Remarque : Remplacez *nom_hôte:numéro_port* dans l'URL par le nom et le port du serveur Web sur lequel réside CA SDM. Toujours dans l'URL, remplacez *nom_hôte_portail:numéro_port_portail* par le nom et le port du serveur Web sur lequel réside le portail.

12. Entrez CA SDM dans la zone de texte Titre.

13. Cliquez sur Avancé.

    La page des propriétés avancées du formulaire de publication de fichier s'ouvre.

14. Entrez *portal/variable-url* dans le champ du type de contenu (MIME), puis cliquez sur Publier.

    Le contenu publié s'affiche dans le dossier Bibliothèque sélectionné.

15. Configurez l'espace de travail pour afficher ce portlet.

16. Déconnectez-vous et reconnectez-vous sous l'identité de l'utilisateur récemment créé. Vous devriez être automatiquement connecté à CA SDM dans le portlet que vous venez de créer sans avoir à vous reconnecter.

Remarque : Lors de l'exécution de CA SDM dans le portlet, l'option Eviter les fenêtres contextuelles n'est pas disponible dans la page Préférence et une fenêtre contextuelle est toujours utilisée quel que soit le paramètre de préférence.

Connexion au serveur CA Portal

Pour vous connecter au serveur CA Portal, ouvrez un navigateur Web et entrez l'URL suivante dans le champ d'emplacement ou d'adresse prévu à cet effet :

```
http://<nom_serveur>:<port#>/servlet/portal
```

<nom_serveur>

Spécifie le nom du serveur (ou l'adresse IP) du serveur du portail.

<port#>

Spécifie le numéro de port que contrôle le serveur CA Portal. Vous avez spécifié le numéro de port durant l'installation du serveur CA Portal. Le port par défaut est 8080.

Configuration de CA SDM pour utiliser SSL avec CA Portal

Remarque : A des fins de production, il est recommandé d'obtenir un certificat auprès d'une autorité de certification approuvée.

Avant de configurer CA SDM pour utiliser SSL, vérifiez si CA Portal et l'intégration de CA SDM fonctionnent sans SSL. Si l'intégration fonctionne sans le SSL, vous pouvez inclure des portlets.

Informations complémentaires :

Intégration de portlets (page 621)

Configuration de SSL à l'aide d'un certificat auto-signé

Pour configurer l'intégration du portail CA SDM à l'aide d'un certificat auto-signé

1. Sur la ligne de commande, entrez :

   ```
   %JAVA_HOME%\bin\keytool -genkey -alias tomcat -keyalg RSA
   ```

   Répondez aux invites de façon appropriée et entrez changeit comme mot de passe en réponse aux deux invites de mot de passe.

   Le certificat est configuré.

2. Modifiez le fichier server.xml à l'emplacement suivant :

   ```
   $NX_ROOT/bopcfg/www/CATALINA_BASE/conf
   ```

3. Supprimez le commentaire de la section suivante et enregistrez :

```
<!--
<Connector className="org.apache.coyote.tomcat4,CoyoteConnector"
   port="8443" minProcessors="5" maxProcessors="75" enableLookups="true"
acceptCount="100" debug="0" scheme="https"
secure="true"useURIValidationHack="false" disableUploadTimeout="true">
<Factory className="org.apache.coyote.tomcat4,CoyoteServerSocketFactory"
clientAuth="false" protocol="TLS" /></Connector>
-->
```

4. Ajoutez l'attribut keystoreFile à server.xml. Lorsque vous exécutez la commande de l'étape 1, un fichier .keystore est créé dans le répertoire de base de l'utilisateur. Ajoutez la référence à l'attribut keystoreFile, puis enregistrez le fichier. Votre fichier server.xml doit se présenter comme suit :

```
<Connector className="org.apache.coyote.tomcat4,CoyoteConnector"

port="8443" minProcessors="5" maxProcessors="75" enableLookups="true"
acceptCount="100" debug="0" scheme="https" secure="true"
useURIValidationHack="false" disableUploadTimeout="true">

<Factory className="org.apache.coyote.tomcat4,CoyoteServerSocketFactory"

clientAuth="false" protocol="TLS" keystoreFile="location/.keystore" />

 </Connector>
```

5. Redémarrez CA SDM.

6. Pour vérifier si SSL fonctionne, pointez votre navigateur vers *https://nom_hôte:8443*. Une alerte de sécurité doit s'afficher. Cliquez sur Oui.

   Remarque : SSL utilise le port 8443.

7. Remplacez le portlet CA SDM pour utiliser HTTPS et le port 8443.

```
https://nom_hôte:8443/CAisd/PortalServlet?

USERNAME=$USER.username$&PORTALSESSION=$SESSION$&PORTALINSTALL=nom_hôte_portail:numéro_port_portail
```

Connexion à CA SDM lorsque CA Portal utilise SSL

Vous pouvez importer le certificat de serveur de CA Portal afin qu'une connexion fiable puisse être effectuée entre CA SDM et CA Portal (lorsque CA Portal est configuré pour utiliser SSL).

Pour se connecter à CA SDM lorsque le portail utilise SSL

1. Vérifiez que CA Portal est configuré et fonctionne avec SSL.

   Remarque : Pour plus d'informations sur le processus de vérification, reportez-vous à la documentation de CA Portal.

2. Exportez le certificat à partir de l'ordinateur sur lequel est installé CA Portal en suivant ces étapes.

   a. Recherchez le fichier server.xml à l'emplacement suivant :

      `PORTAL_Install_Dir\jakarta-tomcat-4.1.29\conf.`

   b. Notez l'emplacement du fichier .keystore et le mot de passe (pwd), comme illustré dans les lignes suivantes de server.xml. Le mot de passe par défaut est *changeit* (tout en minuscule). Si vous avez utilisé un mot de passe personnalisé lors de la création du certificat pendant l'installation du portail, vous devrez utiliser ce mot de passe personnalisé. Pour plus d'informations, reportez-vous à la documentation de CA Portal. Dans les étapes et exemples qui suivent, *changeit* est le mot de passe utilisé par défaut :

      ```
      <!-- Define a SSL Coyote HTTP/1.1 Connector on port 8443 -->
      <Connector className="org.apache.coyote.tomcat4,CoyoteConnector"
         port="8443" minProcessors="5" maxProcessors="150"
            enableLookups="true"
            acceptCount="100" debug="0" scheme="https" secure="true"
            useURIValidationHack="false" disableUploadTimeout="true">
       <Factory className="org.apache.coyote.tomcat4,CoyoteServerSocketFactory"
            keystoreFile="c:\Program Files\CA\SC\Unicenter Management
      Portal\UMPkeystore"
            keystorePass="changeit"
            clientAuth="false" protocol="TLS" />
          </Connector>
      ```

   c. Accédez au répertoire corbeille de JRE (PORTAL_Install_Dir\ jre\bin) sur l'ordinateur du serveur du portail pour accéder à l'utilitaire keytool que vous utiliserez pour exporter le certificat de serveur du portail dans un fichier.

d. Accédez à l'utilitaire keytool, à l'aide de la commande suivante :
```
keytool -export -alias tomcat -file umpserver.cer -keystore "c:\Program Files\CA\SC\Unicenter Management Portal\UMPkeystore"
```
Entrez le mot de passe de l'espace de stockage de la clé : changeit.

Certificat stocké dans le fichier <umpserver.cer>

Remarque : Lorsque vous êtes invité à entrer le mot de passe, veillez à utiliser le mot de passe obtenu à l'étape 2b. Dans l'exemple précédent, le mot de passe noté à l'étape 2b est *changeit*. L'emplacement de keystore est également obtenu à l'étape 2b.

3. Importez le certificat obtenu auprès du serveur sur l'ordinateur qui contient l'installation CA SDM à l'aide de l'utilitaire keytool, comme suit :

a. Sur l'ordinateur CA SDM, accédez au répertoire JRE\bin, qui se trouve en général à l'emplacement suivant :
```
C:\Program Files\CA\SC\JRE\bin.
```

b. Le certificat doit être importé dans l'autorité de certification utilisée par la machine virtuelle Java d'CA SDM.

Voici un exemple d'importation. Dans cet exemple, l'emplacement de l'autorité de certification est :
```
C:\Program Files\CA\SC\JRE\1.4.2_06\lib\security\cacerts
```

Lorsque vous êtes invité à fournir un *mot de passe*, entrez changeit. Lorsque la question *Trust this certificate* (Faire confiance à ce certificat) apparaît, entrez Yes.
```
Keytool.exe -import -alias tomcat -trustcacerts -file umpserver.cer
-keystore "C:\Program Files\CA\SC\JRE\1.4.2_06\lib\security\cacerts"
Entrez le mot de passe de l'espace de stockage de la clé : changeit.
Owner: CN=ump001.ca.com, OU=unicenter, O=ca, L=islandia, ST=ny, C=us
Issuer: CN=ump001.ca.com, OU=unicenter, O=ca, L=islandia, ST=ny, C=us
Serial number: 43ecb469
Valid from: Fri Feb 10 10:42:33 EST 2006 until: Thu May 11 11:42:33 EDT 2006
Certificate fingerprints (Empreintes de certificat) :
         MD5:  A1:AF:AE:92:39:2E:53:D5:1C:6D:FE:44:68:61:DD:5C
         SHA1:
66:3A:BC:77:32:81:60:89:70:B9:EF:FB:74:3D:93:74:CD:8E:E2:D2
Trust this certificate? (Faire confiance à ce certificat ?) [no]:  yes
Certificate was added to keystore (Certificat ajouté au keystore)
```

Remarque : Lorsque vous êtes invité à entrer le mot de passe, utilisez le mot de passe obtenu à l'étape 2b. Dans l'exemple précédent, le mot de passe noté à l'étape 2b est *changeit*.

4. Modifiez le fichier portal-xml-api.xml under $NX_ROOT\bopcfg\www\CATALINA_BASE\webapps\CAisd\WEB-INF\xml\portal-xml-api.xml en effectuant les opérations suivantes :

   a. Remplacez http dans la ligne :
   ```
   <!DOCTYPE PORTAL SYSTEM
   "http://127.0.0.1:8080/servlet/media/xml/api/request.dtd">
   ```

   Par https :
   ```
   <!DOCTYPE PORTAL SYSTEM
   "https://127.0.0.1:8080/servlet/media/xml/api/request.dtd">
   ```

   b. Enregistrez le fichier.

   c. Si Portal_Safe_List a été installé, assurez-vous que vous modifiez le numéro de port en 8443 et le nom de l'ordinateur pour inclure le nom de domaine (par exemple, computername.ca.com:8443).

   Important : Il est important d'inclure le nom de domaine dans le nom de l'ordinateur car le certificat de portail contient le nom de domaine. Pour plus d'informations, reportez-vous à la documentation de CA Portal.

5. Recyclez le serveur CA SDM.

6. A partir de CA Portal, connectez-vous au portlet CA SDM à l'aide de l'URL suivante :

   ```
   http://nom_hôte:numéro_port/CAisd/PortalServlet?USERNAME=$USER.nom_utilisateur$&PORTALSESSION=$SESSION$&PORTALINSTALL=nom_serveur:8443
   ```

   Remarque : Dans l'URL, remplacez *nom_serveur* par le nom du serveur Web sur lequel réside CA Portal. Le nom du serveur dans cette URL doit inclure le nom de domaine, par exemple, nom_serveur.ca.com:8443. Dans l'URL, remplacez nom_hôte:numéro_port par le nom et le port du serveur Web sur lequel réside CA SDM.

Informations complémentaires :

Intégration de portlets (page 621)

Intégration des produits d'ordinateur central

Les données côté serveur CA SDM (fichier .dat) sont associées à des intégrations d'un produit d'ordinateur central.

Charger les données côté serveur CA SDM

Les données côté CA SDM (fichier .dat) associées aux intégrations de produits d'ordinateur central sont répertoriées dans une liste qui associe un fichier .dat au nom du produit d'ordinateur central.

Remarque : Par défaut, le serveur CA SDM est configuré pour utiliser la méthodologie ITIL.

Pour charger des données côté CA SDM pour activer une intégration particulière, utilisez *pdm_userload -f integXXX.dat*.

Les fichiers de données sont livrés dans $NX_ROOT\data\integrations\.

Remarque : Pour plus d'informations sur l'activation du côté appelant (côté produit ordinateur central) de l'intégration, reportez-vous au manuel *CA Common Services for z/OS - CA Service Desk Integration Guide*.

Produits CA utilisant actuellement CAISDI

Le tableau ci-dessous répertorie les produits d'ordinateur central CA qui utilisent actuellement CAISDI et les fichiers .dat associés :

Produit CA	Fichier de données principal	Fichier de mise à jour ITIL
CA Advantage EDBC	integEDBC.dat	
Gestion des bandes CA 1	integCA1.dat	itil_integCA1.dat
CA Allocate DASD Space and Placement	integAllocate.dat	itil_integAllocate.dat
CA Disk Backup and Restore	integDisk.dat	itil_integDisk.dat
CA TLMS Tape Management (CA TLMS)	integTLMS.dat	itil_integTLMS.dat
CA Vantage Storage Resource Manager (CA Vantage SRM)	integVantage.dat	itil_integVantage.dat
CA 7 Workload Automation (CA 7 WA)	integCA7.dat	itil_integCA7.dat
CA JARS Resource Accounting (CA JARS RA)	integJARS.dat integJARSMVS.dat	itil_integJARS.dat itil_integJARSMVS.dat
CA MIM Resource Sharing (CA MIM RS)	integMIM.dat	itil_integMIM.dat
CA OPS/MVS Event Management and Automation (CA OPS/MVS EMA)	integOPSMVS.dat	itil_integOPSMVS.dat
CA SYSVIEW Performance Management (CA SYSVIEW)	integSysview.dat	itil_integSysview.dat

CA NetMaster Network Management for TCP/IP (CA NetMaster NM for TCP/IP)	integNetMaster.dat	itil_integNetMaster.dat
CA NetMaster Network Management for SNA (CA NetMaster NM for SNA)	integNetMaster.dat	itil_integNetMaster.dat
CA NetMaster Network Automation (CA NetMaster NA)	integNetMaster.dat	itil_integNetMaster.dat
CA NetMaster	integNetMaster.dat	itil_integNetMaster.dat
CA NetMaster Network Operations for TCP/IP (CA NetMaster NO for TCP/IP)	integNetMaster.dat	itil_integNetMaster.dat
CA NetMaster File Transfer Management (CA NetMaster FTM)	integNetMaster.dat	itil_integNetMaster.dat
CA MICS Resource Management (CA MICS)	integNeuMICS.dat	itil_integNeuMICS.dat

Produits CA susceptibles d'utiliser CAISDI

Le tableau qui suit répertorie les produits d'ordinateur central CA susceptibles d'utiliser CAISDI et les fichiers .dat associés :

Produit CA	Fichier de données principal	Fichier de mise à jour ITIL
CA 2E	integ2e.dat	
CA Enterprise Workload Automation	integAutoSys.dat	
CA Bundl	integBundl.dat	
CA 11 Enterprise Workload Automation Restart and Tracking	integCA11.dat	
Conn CA	integConnect.dat	
CA Datamacs	integDatamacs.dat	
CA Date Simulator	integDate.dat	
CA Deliver	integDeliver.dat	itil_integDeliver.dat
CA Dispatch	integDispatch.dat	itil_integDispatch.dat
CA FAVER VSAM Data Protection	integFaver.dat	
CA FileAge	integFileAge.dat	
CA File Master Plus	integFileMaster.dat	
CA Filesave RCS Automated Recovery	integFileSave.dat	
CA Gen	integGen.dat	
CA GSS (composant commun)	integGSS.dat	

CA InterTest	integInterTest.dat	
CA JCLCheck Enterprise Workload Automation	integJCLCheck.dat	
CA Jobtrac Job Management	integJobtrac.dat	itil_integJobtrac.dat
CA LPD Report Convergence	integLPD.dat	
CA Optimizer	integOptimizer.dat	
CA Optimizer/II	integOptimizerII.dat	
CA Plex	integPlex.dat	
CA Scheduler Job Management	integScheduler.dat	
CA Spool Enterprise Print Management	integSpool.dat	itil_integSpool.dat
CA SymDump	integSymDump.dat	
CA Verify	integVerify.dat	
Vue CA	integView.dat	itil_integView.dat

Intégration de CA Business Service Insight

CA Business Service Insight (CA BSI) permet de gérer des performances de services informatiques, telles que l'intégration de service et la gestion des performances de niveau de service, ainsi que l'exploitation des évaluations et des comparaisons de service. CA BSI permet à votre organisation de déterminer le fonctionnement des services en fonction des accords sur les niveaux de service (SLA). CA BSI fournit des informations sur la gestion des niveaux de service aux analystes du centre de services dans CA SDM pour gérer les changements apportés aux divers services informatiques de votre organisation. Ces informations sur la gestion des niveaux de service permettent une meilleure prise de décision et une livraison de services informatiques améliorée.

L'intégration de CA BSI ajoute des onglets qui apparaissent dans des formulaires détaillés d'élément de configuration dans CA SDM. Les rapports de conformité des niveaux de service et de niveau de service modifié par mesures/cible fournissent des informations sur les éléments de configuration de famille Service d'entreprise CA SDM. Le rapport de niveau de service modifié par contrat/cible fournit des informations sur les éléments de configuration de famille Contrat CA SDM.

Remarque : Ces onglets s'affichent uniquement pour des CI comprenant des mappages d'actifs fédérés au RDG CA BSI.

Lorsque vous intégrez CA SDM avec CA BSI, les utilisateurs peuvent afficher les données de mesure pour les CI de contrat associés à un RDG CA BSI. Les utilisateurs doivent spécifier un contractant (entité CA BSI) avant de soumettre la demande. Une restriction de CA BSI empêche les données de mesure d'être correctement affichées pour les contractants dont le nom contient certains caractères non alphanumériques. Il est recommandé d'utiliser des noms de contractant contenant uniquement des caractères alphanumériques et d'éviter les caractères suivants :

reserved = gen-delims / sub-delims

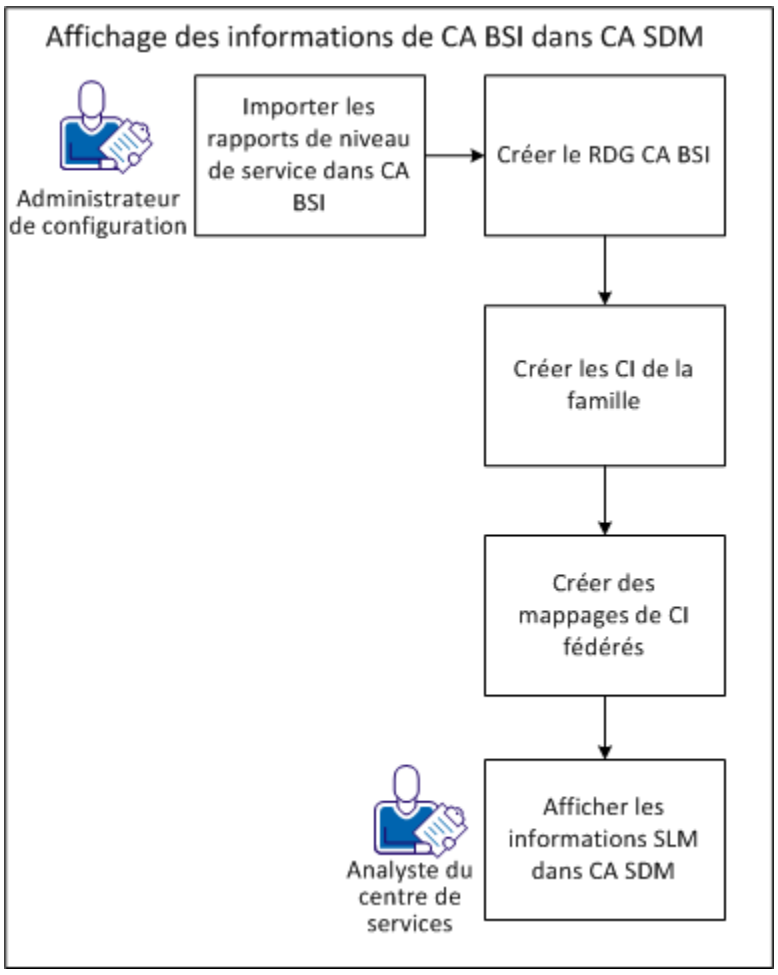
gen-delims = : / ? # [ ] @

sub-delims = ! $ & ' ( ) * + , ; =

Affichage des informations de CA BSI dans CA SDM

Une organisation souhaite améliorer la gestion des changements apportés aux services informatiques et décide d'intégrer CA BSI et CA SDM. L'intégration permet à CA BSI d'exporter les informations sur la gestion des niveaux de service (SLM) vers CA SDM. L'administrateur de configuration importe les rapports dans CA BSI et configure CA SDM de sorte qu'un analyste du centre de services puisse afficher les informations SLM. Les analystes du centre de services utilisent ces informations pour améliorer la livraison de services informatiques.

Le diagramme suivant illustre l'activation par un administrateur de configuration de CA BSI pour exporter des données SLM dans CA SDM de sorte qu'un analyste du centre de services puisse afficher les informations :


Affichage des informations de CA BSI dans CA SDM
Administrateur de configuration
Importer les rapports de niveau de service dans CA BSI
Créer le RDG CA BSI
Créer les CI de la famille
Créer des mappages de CI fédérés
Analyste du centre de services
Afficher les informations SLM dans CA SDM

1. Importation des rapports de niveaux de service dans CA BSI (page 633)
2. Création du RDG CA BSI (page 633)
3. Création des CI de famille (page 634)

4. Création des mappages de CI fédérés (page 635)
5. Affichage des informations de SLM dans CA SDM (page 636)

Importation des rapports de niveaux de service dans CA BSI

CA BSI fournit le rapport de *conformité des niveaux de service* par défaut. L'onglet Service BSI s'affiche dans des pages de détail d'éléments de configuration dans CA SDM et contient le nombre de dépassements et de violations. Importez les rapports de *niveau de service modifié par métrique/cible* et *niveau de service modifié par contrat/cible* dans CA BSI.

1. Copiez le fichier $NX_ROOT/samples/BSI/bsireports.sql dans le serveur de base de données CA BSI.

   Ce script Oracle contient les définitions de rapport requises pour l'intégration entre CA BSI et CA SDM.
2. Connectez-vous à l'instance Oracle de CA BSI avec un utilisateur disposant du rôle SYSDBA, ou connectez-vous en tant que propriétaire de base de données.

   Important : Cet utilisateur *doit* disposer de droits de mise à jour de la base de données. Confirmez auprès de votre administrateur de base de données Oracle si vous disposez de ces droits.
3. Exécutez le script bsireports.sql et vérifiez qu'aucune erreur ne se produit.

   Les rapports sont disponibles pour l'intégration CA SDM.

Création du RDG CA BSI

L'administrateur de configuration crée un RDG pour CA BSI dans CA SDM. Ce RDG fournit des informations concernant le serveur CA BSI, telles que le nom d'hôte et l'ID d'utilisateur privilégié.

1. Dans l'onglet d'Administration, accédez à CA CMDB, Gestion RDG, Liste des RDG.
2. Cliquez sur Créer.
3. Renseignez les exemples d'informations suivants :
   - Entrez **BSI** comme nom de classe.
   - Entrez des étiquettes pour les noms de bouton et RDG.

     Par exemple, entrez **BSI**.

- Spécifiez le nom d'hôte du serveur CA BSI.
- Entrez **sadmin** en tant qu'ID utilisateur et **CA** comme secret partagé.

  Remarque : Ces informations dépendent de votre nom d'utilisateur et de votre organisation. Confirmez ces informations auprès de votre administrateur CA BSI.
- Supprimez tout le contenu du champ URL à lancer en contexte.

4. Cliquez sur Enregistrer et fermez la fenêtre.

Créez les CI dans CA SDM.

Créez les CI Service d'entreprise et Famille Contrat dans CA SDM. Ces CI correspondent à des données de CA BSI que vous voulez afficher dans CA SDM. Dans cet exemple, vous créez le Service 1 et le Contrat 7.

1. Dans l'onglet Administration, cliquez sur CA CMDB, Liste des CI.
2. Cliquez sur Créer.
3. Spécifiez les informations suivantes :
   - Entrez **Service 1** comme nom.
   - Entrez **Service commercial** comme classe.
4. Cliquez sur Continuer.
5. Cliquez sur Enregistrer et fermez la fenêtre.
6. Créez un autre CI avec les informations suivantes :
   - Entrez **Service 7** comme nom.
   - Entrez **Contrat de licence** comme classe.
7. Cliquez sur Continuer.
8. Cliquez sur Enregistrer et fermez la fenêtre.

Création de mappages de CI fédérés

Créez des mappages de CI fédérés pour effectuer l'intégration entre CA BSI et CA SDM. Ce mappage fournit des informations concernant un élément de configuration. Dans cet exemple, vous mappez le Service 1 et le Contrat 7 vers le RDG BSI.

1. Dans l'onglet Administration, cliquez sur CA CMDB, Gestion du RDG gestion, Mappage des éléments de configuration fédérés.
2. Cliquez sur Créer.
3. Remplissez les champs suivants :
   - Entrez **Service 1** comme nom de CI et ID d'actif fédéré.
   - Entrez **BSI** comme nom de RDG.

   Important : Veillez à entrer le même ID d'actif fédéré que les noms de service et de contrat dans CA BSI.
4. Cliquez sur Enregistrer et fermez la fenêtre.
5. Créez un autre mappage et remplissez les champs suivants :
   - Entrez **Service 7** comme nom de CI et ID d'actif fédéré.
   - Entrez **BSI** comme nom de RDG.
6. Cliquez sur Enregistrer et fermez la fenêtre.

Affichage des informations de SLM dans CA SDM

L'analyste du centre de services affiche les informations de SLM pour gérer les changements apportés aux services informatiques dans votre organisation. Par exemple, vous voulez analyser les violations qui apparaissent pour le Service 1.

1. Dans l'onglet Administration, cliquez sur CA CMDB, Liste des CI.
2. Recherchez les CI de famille de service d'entreprise et de contrat que vous avez intégrés à CA BSI.
3. Ouvrez un CI de famille de service d'entreprise pour afficher les onglets Service BSI et Service BSI par métrique.
4. Cliquez sur Service BSI pour afficher les informations de dépassement et de violation des *données de conformité des niveaux de service* dans CA BSI.

   Les données de dépassement et de violation du rapport de *conformité des niveaux de service* de CA BSI s'affichent pour Service 1.
5. Cliquez sur Service BSI par métrique pour afficher le rapport de métrique, violation, conformité et cible à partir des données *Niveau de service modifié par métrique/cible* dans CA BSI.
6. Ouvrez un CI de famille de contrat intégré à CA BSI et cliquez sur l'onglet Contrat BSI par onglet.

   Remarque : Les CI de contact contiennent l'onglet Contrat de BSI par métrique. Cet onglet contient une zone de texte dans laquelle vous entrez le contractant du Contrat pour récupérer des informations du rapport *Niveau de service modifié par contrat/cible* dans CA BSI.

Vous avez correctement intégré CA BSI à CA SDM pour afficher des informations de SLM dans CA SDM.

Chapitre 14: Répertoire Samples

Ce chapitre traite des sujets suivants :

Contenu du répertoire Samples (page 637)

Contenu du répertoire Samples

Vous pouvez modifier plusieurs fichiers dans le répertoire $NX_ROOT/samples afin de les utiliser dans diverses interfaces externes. Ces fichiers sont regroupés dans divers sous-répertoires. Aucun des fichiers figurant dans le répertoire Samples ne sont livrés au départ en tant que fichiers exécutables.

Modification du catalogue de messages

Pour modifier le catalogue de messages, effectuez les opérations suivantes :

1. Reportez-vous au format de pdm.xml situé dans $nx_root\bin.
2. Créez une copie personnalisée de pdm.xml et placez-la dans le répertoire $nx_root\msg_catalog.
3. Ajoutez, modifiez ou ajoutez et modifiez des messages dans les fichiers de messages XML présentés à l'étape précédente.

call_mgt

Contient des exemples de personnalisation de gestion des appels.

gencr.frg

Vous pouvez utiliser ce fichier en association avec la commande bop_cmd pour créer des appels à partir d'une ligne de commande. Toutes les notifications et les entrées du journal d'activité apparaissent normalement, mais aucun formulaire d'appel ne s'affiche sur le serveur lors de la création. Vous devez utiliser le paramètre -u pour exécuter gencr.frg avec l'utilitaire bob_cmd. Veillez à consulter le fichier gencr_readme.txt pour vous familiariser avec la syntaxe et savoir comment la modifier si nécessaire. Vous devez placer le fichier dans $NX_ROOT/site/mods/interp. Si ce répertoire n'existe pas, créez-le. Exemple : bop_cmd -d domsrvr -u nsm -f gencr.frg "gencr ('Ma description')"

iss_site.mod

Vous pouvez utiliser ce fichier pour activer la journalisation des activités des champs adaptés aux sites dans les demandes client. Vous devez placer ce fichier dans le répertoire $NX_ROOT/site/mods/majic après l'avoir modifié pour les champs adaptés aux sites.

cr_site.mod

Vous pouvez utiliser ce fichier pour activer la journalisation des activités des champs adaptés aux sites dans les appels. Vous devez placer ce fichier dans le répertoire $NX_ROOT/site/mods/majic après l'avoir modifié pour les champs adaptés aux sites.

chg_site.mod

Vous pouvez utiliser ce fichier pour activer la journalisation des activités des champs adaptés aux sites dans les demandes de changement. Vous devez placer ce fichier dans le répertoire $NX_ROOT/site/mods/majic après l'avoir modifié pour les champs adaptés aux sites.

gencr_readme.txt

Ce fichier contient des instructions sur l'utilisation du fichier gencr.frg.

chg_site.spl

Vous pouvez modifier ce fichier pour modifier le mappage des attributs lorsque vous créez une demande de changement à partir d'une demande. Vous devez placer ce fichier dans le répertoire $NX_ROOT/site/mods/majic après avoir effectué les modifications appropriées.

audlog_site.mod

Vous pouvez utiliser ce fichier pour activer la journalisation de vérification des champs adaptés aux sites. Vous devez placer ce fichier dans le répertoire $NX_ROOT/site/mods/majic après l'avoir modifié pour les champs adaptés aux sites.

Notify_add.spl (UNIX uniquement)

Vous pouvez utiliser ce fichier pour ajouter l'agent de journalisation, la personne assignée et le groupe de l'appel à la liste des notifications de l'appel. Ce fichier doit être placé dans le répertoire $NX_ROOT/site/mods/majic.

Notify_replace.spl (UNIX uniquement)

Vous pouvez utiliser ce fichier pour ajouter l'agent de journalisation, la personne affectée et le groupe de l'appel à la liste des notifications de l'appel si vous avez modifié ces éléments. Ce fichier doit être placé dans le répertoire $NX_ROOT/site/mods/majic.

data

Ce répertoire contient des fichiers décrivant le modèle de données logique pour la plupart des tables de base de données dans CA SDM. Ce répertoire de données inclut également des exemples de données pour Gestion des connaissances.

macro_lock

Ce fichier contient un fragment SPEL que vous pouvez exécuter à l'aide d'une commande bop_cmd pour désactiver les verrous imposés par les macros.

hébergement multiclient

Ce répertoire contient des fichiers exemples pour l'administration de l'hébergement multiclient.

Renseignements supplémentaires :

Conversion d'une mise en oeuvre de client hébergé existante en objet de client hébergé (page 325)
Remplissage des attributs de client hébergé dans vos tables (page 326)

pdmconf

web.xml.tpl

pdm_startup.tpl

pdm_edit_usage_notes.htm

alias_install.bat

web.cfg.tpl

pdm_startup.i.tpl

pdm_edit.pl

README_files

Tous ces fichiers sont utilisés par pdm_edit.pl pour la création de fichiers de démarrage destinés à un serveur principal et à des serveurs secondaires configurés pour l'exécution de divers démons.

signalement

Ce répertoire contient de la documentation et des exemples pour configurer le signalement hors ligne.

Renseignements supplémentaires :

Base de données répliquée pour le signalement hors ligne (page 266)

sdk

Ce répertoire contient un exemple de fichier permettant d'effectuer des appels du service Web SOAP CA SDM.

Le fichier TableOfContents.doc indique les éléments disponibles, trouvés dans le répertoire suivant :

$NX_ROOT\samples\sdk\websvc

Les fichiers PKI_loginServiceManaged_JAVA_steps.doc et PKI_loginServiceManaged_PERL_steps.doc expliquent comment configurer CA Service Desk pour les connexions de certificat numérique dans le répertoire suivant :

$NX_ROOT\samples\sdk\websvc\java\test1_pki

Vous trouverez ci-dessous une liste de modèles, d'exemples et d'emplacements PERL et JAVA :

- Exemples PERL

  $NX_ROOT\samples\sdk\websvc\perl\test1_pki

  Exemple : appel de service Web loginServiceManaged()

- Exemples JAVA

  $NX_ROOT\samples\sdk\websvc\java\test1_pki

  Exemple : appel de service Web loginServiceManaged() et getBopsid()

  $NX_ROOT\samples\sdk\websvc\java\test2_basic

  Exemple : appel de service Web combiné CreateRequest() et CreateChangeOrder()

vues

Ce répertoire contient des scripts de base de données utilisés pour la migration, l'administration de l'hébergement multiclient et d'autres processus.

Chapitre 15: Chargement de contenu supplémentaire

Ce chapitre traite des sujets suivants :

sd_content.dat (page 643)

sd_content.dat

Du contenu supplémentaire pour CA SDM est disponible dans sd_content.dat. Ce fichier de données contient des enregistrements Catégorie de changement et Cause première. Pour charger les données à partir d'une fenêtre de commande, accédez à $NX_ROOT/data et exécutez la commande suivante.

```
pdm_load –f sd_content.dat
```